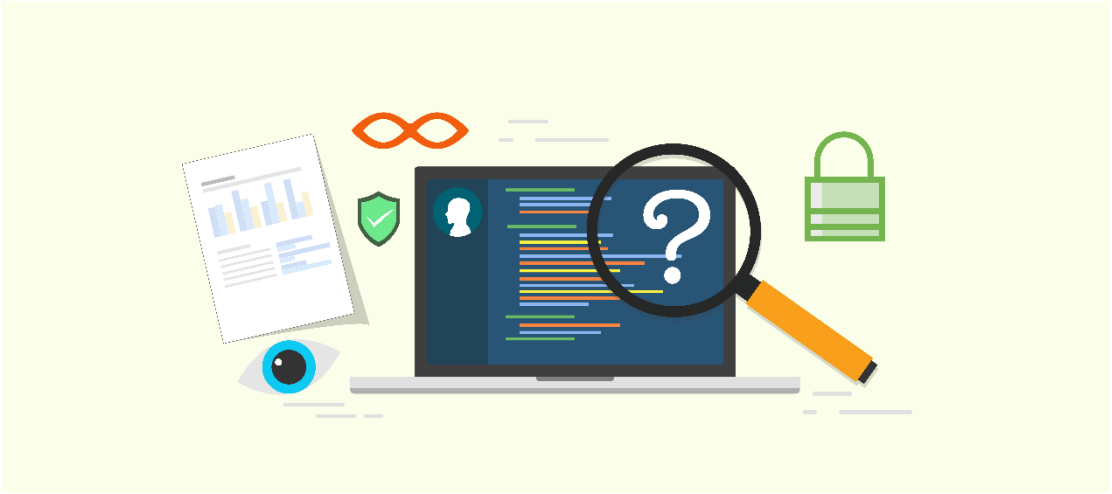
STUDY

Requested by the LIBE committee

European Parliament

An assessment of the Commission's proposals on electronic evidence



Policy Department for Citizens' Rights and Constitutional Affairs
Directorate General for Internal Policies of the Union
PE 604.989 - September 2018

EN

An assessment of the Commission's proposals on electronic evidence

STUDY

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, analyses the added value and the shortcomings of the Commission's proposals on cross-border access to electronic evidence, with a special focus on the proposals' implications for territoriality and state sovereignty and fundamental rights of service providers and users.

ABOUT THE PUBLICATION

This research paper was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs and was commissioned, overseen and published by the Policy Department for Citizen's Rights and Constitutional Affairs.

Policy Departments provide independent expertise, both in-house and externally, to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU external and internal policies.

To contact the Policy Department for Citizens' Rights and Constitutional Affairs or to subscribe to its newsletter please write to: poldep-citizens@europarl.europa.eu

RESPONSIBLE RESEARCH ADMINISTRATOR

Kristiina MILT
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@europarl.europa.eu

AUTHOR

Prof. Martin BÖSE, Professor, Rheinische Friedrich-Wilhelms-Universität Bonn

LINGUISTIC VERSION

Original: EN

Manuscript completed in September 2018

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
Art.	Article / Articles
CCC	Convention on Cybercrime
CFR	Charter of Fundamental Rights of the European Union
CISA	Convention Implementing the Schengen Agreement
CJEU	Court of Justice of the European Union
ECHR	European Convention on Human Rights
EIO	European Investigation Order
EPOC	European Production Order (Certificate)
EPOC-PR	European Preservation Order (Certificate)
EU	European Union
JHA	Justice and Home Affairs
MLA	Mutual Legal Assistance
MS / MSs	Member State / Member States
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
US	United States of America

EXECUTIVE SUMMARY

Background

Internet-based information and communication systems (e-mail, social media, messaging apps, cloud computing systems) have become integral part of everyday life. Accordingly, access to electronic data processed and stored by service providers has increasingly gained in importance in criminal investigations. As provider data is often stored on and moved between servers located in several jurisdictions, access to such data usually requires a request for mutual legal assistance (MLA). The traditional framework of international cooperation in criminal matters, however, bears the risk that the data may have been deleted or transferred before the requested state decides to take action. As an alternative to MLA proceedings, a practice of direct cooperation requests to service providers has emerged. This practice, however, relies upon the provider's willingness to cooperate and, thus, does not ensure effective and equal access to the relevant data.

In order to meet these challenges, the Commission proposed on 17 April 2018 new rules on cross-border access to electronic evidence, namely a regulation on European Production and Preservation Orders for electronic evidence in criminal proceedings and a directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. By these proposals, the Commission responds to the Council's and the European Parliament's calls for a common EU approach in this field.

Aim

The aim of this study is to assess whether the new rules proposed by the Commission provide an adequate and feasible framework for cross-border access to provider data. To that end, the study shall analyse the added value and shortcomings of the Commission's proposal and assess the legal implications of the transnational disclosure of provider data, with a special focus on the disparities of national legal systems and recent developments concerning access to evidence stored in other jurisdictions, the legal challenges as regards territorial sovereignty and fundamental rights protection as well as the possibilities offered by Mutual Legal Assistance agreements and mutual recognition instruments.

Findings

The international framework of cross-border access to provider data mainly relies on MLA proceedings. In the EU, the European Investigation Order has significantly facilitated cross-border cooperation by streamlining the procedure and reducing cooperation obstacles, but still requires an intervention of the MS where the investigative measure shall be executed. In contrast, the Commission's proposal will create new instruments for direct and mandatory cross-border cooperation, namely the European Production Order (EPOC) and the European Preservation Order (EPOC-PR). The orders are addressed to the legal representative to be designated by any service provider offering its services in the Union. The role of the formerly executing MS is limited to the enforcement of the order if the addressee does not comply with its obligations.

The added value of the new cooperation regime lies in providing quick and effective cross-border access to provider data. On the other hand, the Commission's proposal suffers from major shortcomings:

- The Commission's proposal extends enforcement jurisdiction to service providers established and data stored in non-Member States and thereby compromises the functioning of international cooperation with third states and gives rise to legal uncertainty for both service providers and users.
- Direct cooperation will affect the territorial sovereignty of the MS in which the service provider shall execute the EPOC or the EPOC-PR and will, thereby, prevent that MS from taking responsibility for an effective protection of fundamental rights within its territory. Instead, the protective function is shifted to the service provider and/or the competent authority of the issuing MS neither of which is in position to ensure adequate protection.
- The proposed cooperation mechanism deprives the individual of the protection provided by the traditional framework of international cooperation by abolishing traditional cooperation obstacles (for instance the double criminality requirement). Most of all, the proposal establishes an obligation to produce content data and transactional data even if the threshold set out by the law of the enforcing MS is not met (serious offence, catalogue offence).
- As a consequence of the re-allocation of protective functions among the issuing and the enforcing MS, the individual whose data has been transmitted has no right to challenge the disclosure before a court of the enforcing MS. The service provider is provided with judicial remedies in the enforcing MS (enforcement proceedings) and in the issuing MS (review procedure in case of conflicting obligations), but may not challenge the legality of the order under the law of the issuing MS.
- The Commission's proposal will not fully overcome the fragmentation and divergence of the MSs' laws on the preservation and production of electronic evidence. Production and preservation orders to domestic service providers will remain subject to national law and the proposed cooperation regime still significantly refers to the national laws of the issuing and enforcing MS.

Recommendations

To address the shortcomings of the new cooperation regime proposed by the Commission, this study recommends

- to re-consider whether and to what extent recourse to the EIO might be an alternative option to the EPOC or the EPOC-PR (in particular with regard to the disclosure of content and transactional data);
- to coordinate the legislative proposal with bi- and multilateral agreements and to limit unilateral enforcement jurisdiction by a connecting factor that is strictly construed and provides legal certainty for service providers and users;
- to strengthen the role of the enforcing MS by a notification mechanism that enables its competent authority to take a decision on the execution of the order;
- to maintain the high standards of protection established in the framework of cross-border cooperation in the AFSJ and provided by the law of the enforcing MS (in particular the thresholds for accessing content data and transactional data);
- to ensure effective judicial review by providing legal remedies in both the issuing and the enforcing MS and enabling the service provider to challenge the legality of the EPOC / the EPOC-PR in the issuing MS.

1. INTRODUCTION

1.1. Background

Due to the widespread use of modern information and communication technology, electronic evidence stored on computer systems has increasingly gained in importance in criminal investigations. Communication systems (webmail, messaging apps etc.) produce a huge amount of data that may be potentially relevant in criminal proceedings. Since these data are processed, transferred and stored by service providers, their disclosure and production to law enforcement authorities has become a key element in criminal investigations.

In cross-border cases, there are basically three means to obtain access to provider data. The traditional instrument is provided by the rules of **mutual legal assistance (MLA)**. According to these rules, the state where the service provider is established is requested to collect and transfer the electronic evidence to the competent authority of the requesting state. MLA proceedings, however, consume both time and resources and, thereby, may hamper effective and quick access to electronic evidence.

The second instrument avoids time-consuming MLA-proceedings and relies on **direct cooperation with foreign service providers**. This model has become most relevant with regard to the main service providers established in the USA: In 2016, law enforcement authorities of the MSs issued more than 120.000 cooperation requests to Apple, Facebook, Google, Microsoft, and Twitter.[1] Request-based cooperation with service providers, however, depends on the provider's willingness to cooperate and the respective company's policy.

The third means relies on mandatory instead of voluntary cooperation. Some states have established an **obligation of foreign service providers to disclose** relevant data irrespective of the location where the data is stored or processed, and thereby extended their **enforcement jurisdiction** to any provider offering electronic communication services within their territory.[2] This may even extend to direct access without involvement of the service provider (for instance by online searches). Other countries, however, adhere to a stricter understanding of territorial sovereignty and have not extended their jurisdiction to data stored abroad.

The shortcomings and the diversity of the existing rules and practices on cross-border access to provider data were addressed by the Council's conclusions on improving criminal justice in cyberspace of 9 June 2016 in which the **Council** requested the Commission to develop a common EU approach that should be based on the following guidelines related to the instruments mentioned above:

- streamlining MLA proceedings for obtaining electronic evidence;
- enhancing direct cooperation with service providers or any other solution that allows for a quick disclosure of data;
- review of connecting factors that could provide grounds for enforcement jurisdiction.[3]

[1] Commission, Staff Working Document, Impact Assessment, SWD (2018) 118 final, 17 April 2018, p. 15.
[2] Art. 46bis of the Belgian Code of Criminal Procedure; for the application to foreign providers see the judgment of the Hof van Cassatie [Belgian Court of Cassation], Judgment of 1 December 2015, P.13.2082.N, Yahoo.
[3] Council, Conclusions on improving criminal justice in cyberspace, Council doc. No. 10007/16, 9 June 2016, p. 5 ff.

In December 2016, the **Commission** presented a **non-paper** in which the problems linked to the existing framework were elaborated in further detail:[4]

- MLA proceedings were considered as unsuitable for accessing electronic data which is volatile in nature and may have been deleted or transferred before the requested state decides to take action. Furthermore, MLA proceedings were considered resource-intensive and complex and, thus, unnecessarily onerous and intransparent. According to the Commission, these objections even applied to mutual recognition instruments (the European Investigation Order).
- As regards direct cooperation with service providers, the Commission established a lack of transparency and legal certainty originating from different company policies or practices (criteria and time-frames for disclosure) and divergent national legislation (notification of users, request formats, accountability and liability of service providers). This variety had led to significantly different rates of disclosure of the requested data, depending on the requesting MS and the requested provider. In addition, the law enforcement authorities reported problems in identifying and contacting the relevant service provider respectively its contact point.
- According to the Commission, MSs followed divergent approaches on establishing enforcement jurisdiction for obtaining access to provider data (jurisdiction based on the location of data, the establishment of service providers, the place where the provider was offering services, the nationality of the person the electronic data pertained to), and this fragmentation created legal uncertainty for both the providers and the individuals concerned. Furthermore, reference to the place where the data is stored or processed might confront the law enforcement authorities with serious problems if the data is moved between servers in varying locations or – as in cloud computing systems – is even scattered over several jurisdictions that are unknown to users and law enforcement authorities ("loss of location").[5] On the other hand, extending jurisdiction to foreign service providers and data stored abroad might turn out insufficient if the production order could not be enforced.

On the basis of its interim report, the Commission discussed potential legislative solutions in a further non-paper[6] and a **technical document**[7]. In these documents, the Commission shaped a legal framework for voluntary or mandatory cooperation with foreign services providers, but also elaborated on modalities for direct cross-border access to electronic evidence without cooperation of a foreign service provider being necessary (hacking, extended searches etc.).[8]

In its resolution of 3 October 2017 on the fight against cybercrime, **European Parliament** called on the Commission to put forward a new framework for e-evidence, including harmonised rules to determine the status of a provider as domestic or foreign, and to impose an obligation on service providers to respond to requests from other Member States that are based on due legal process and in line with the European Investigation Order (EIO), while taking account of the principle of proportionality to avoid

[4] Commission, Non-paper: Progress report following the Conclusions of the Council of the European Union on improving criminal justice in cyberspace, Council doc. No. 15072/16, p. 6 ff.
[5] See also Cybercrime Convention Committee (T-CY), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, Transborder access and jurisdiction: What are the options?, Report of the Transborder Group, adopted by the T-CY on 6 December 2012, T-CY (2012)3, para. 31 f.
[6] Commission, Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, 22 May 2017 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf (31 August 2018).
[7] Commission, Technical document: Measures to improve cross-border access to electronic evidence for criminal investigations following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace, Council doc. No. 9542/17, 22 May 2017.
[8] Commission, Technical document (note 7), pp. 28 ff., 37 ff.

adverse effects on the exercise of the freedom of establishment and the freedom to provide services and ensuring adequate safeguards and legal certainty.[9]

On 17 April 2018, the **Commission proposed** a **Regulation** on European Production and Preservation Orders for electronic evidence in criminal proceedings[10] and a **Directive** laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings[11]. In these proposals, the Commission did not pursue the idea of direct cross-border access to provider data, but focused on a new framework for **mandatory cross-border cooperation with service providers**. To that end, the Commission's proposals created two new cooperation instruments, namely the **European Production Order Certificate (EPOC)** and the **European Preservation Order Certificate (EPOC-PR)** and provided for an obligation of service providers to designate a legal representative in the Union for the receipt of, compliance with and enforcement of the new cooperation instruments.

1.2. Study objectives and outline

The overall objective of this study is to assess the Commission's proposals on electronic evidence to support the legislative report of the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee). Thus, the main aim is to assess whether the new rules proposed by the Commission provide an adequate and feasible framework for cross-border access to electronic evidence. In particular, the study shall

- analyse the added value and shortcomings of the Commission's legislative proposals in the light of the recommendations of the European Parliament resolution of 3 October 2017 on the fight against cybercrime;
- assess the legal implications of the transnational access to provider data, thereby taking into account the disparities of national legal systems and recent developments concerning access to electronic evidence stored in other jurisdictions, the legal challenges as regards territoriality and sovereignty and fundamental rights protection as well as the possibilities offered by Mutual Legal Assistance agreements and mutual recognition instruments.

To address these issues, the study is structured as follows:

Section 2 will describe the existing international and EU framework of cross-border access to electronic evidence, in particular the Council of Europe Convention on Cybercrime and the European Investigation Order.

Section 3 shall analyse the new rules proposed by the Commission, thereby focussing on the changes and differences from the current legal framework.

Section 4 will address the matter of enforcement jurisdiction and territorial sovereignty. The extraterritorial dimension of the new instruments is twofold: On the one hand, the order obliges the addressee to produce (or preserve) data even if it is stored on a server located in a foreign jurisdiction.

[9] European Parliament, Resolution on the fight against cybercrime (2017/2068(INI)), P8_TA(2017)0366, 3 October 2017, para. 64.
[10] Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings, COM (2018) 225 final, 17 April 2018.
[11] Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM (2018) 226 final, 17 April 2018.

On the other hand, the new instrument will create a transnationally binding obligation of its addressee and thereby fundamentally differ from the current legal framework of cross-border cooperation.

Section 5 will focus on fundamental rights, the right to privacy in particular, and examine whether the new rules provide for an adequate level of protection, strong procedural safeguards and effective legal remedies. Furthermore, this section shall discuss whether the European regime will overcome the fragmentation of divergent national laws and, thereby, improve legal certainty for businesses and service providers.

Section 6 will present the main conclusions to be drawn from this study and provide policy recommendations for amendments to the Commission's proposal.

2. CROSS-BORDER ACCESS TO PROVIDER DATA – THE STATUS QUO

KEY FINDINGS

- The international framework of cross-border access to provider data mainly relies on the Council of Europe Convention on Cybercrime. The Convention lays down minimum requirements on investigative measures, including production orders and preservation orders. According to the Cybercrime Committee, the jurisdiction to enforce such orders is not necessarily linked to the location where the data is stored, but may also be determined by the place where the provider is offering its services. The treaty provisions on international cooperation rely on the traditional MLA framework; nevertheless, the Convention provides for several practical measures to enhance cooperation and special provisions on the expedited preservation of stored computer data and direct cross-border access to computer data stored abroad.

- In the EU, the traditional MLA framework for transnational evidence-gathering has been replaced by the European Investigation Order that has significantly facilitated cross-border cooperation by streamlining the procedure and reducing cooperation obstacles. Nevertheless, the mechanism still requires a decision of another MS to recognise and execute the production order. Unlike the Cybercrime Convention, EU law does not provide for direct cross-border access to electronic evidence.

The added value and the shortcomings of the Commission's proposals on cross-border access to provider data cannot be assessed without taking into account the existing legal framework on access to electronic evidence that, according to the Commission, were not considered to provide adequate means to effectively access electronic evidence stored in a foreign jurisdiction. The following subsections will provide an overview of the traditional framework of mutual legal assistance established by international treaty law (2.1.) and the corresponding EU legislation implementing the principle of mutual recognition (2.2.) and shall examine whether and to what extent the Commission's concerns are justified.

2.1. International treaty law: The Convention on Cybercrime

In situations where electronic evidence is stored abroad, international treaties provide for general rules on request-based cross-border access to any evidence (including data) located in the requested state. This general framework established by MLA treaties (such as the European Convention on MLA[12]) has been further developed by the Council of Europe Convention on Cybercrime (CCC)[13] that entails specific rules for access to electronic evidence. The Cybercrime Convention has been ratified by most MSs (except for Ireland and Sweden) and several non-European countries, in particular the US.[14] The treaty provisions address both domestic and cross-border access to computer data.

2.1.1. Common provisions on access to provider data

In order to enable law enforcement authorities to successfully investigate cybercrime and to adapt the national procedural laws to the new technological developments, the Convention entails minimum

[12] European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 (ETS No. 30).
[13] Convention on Cybercrime of 23 November 2001 (ETS No. 185).
[14] See the chart of signatures and ratifications https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=w8r6xLCC (31 August 2018).

requirements on investigative powers available in a criminal investigation. In particular, the State Parties shall provide for the following investigative measures to secure and collect electronic evidence:

- expedited preservation of stored computer data (Art. 16 CCC);
- expedited preservation and partial disclosure of traffic data (Art. 17 CCC);
- production orders (Art. 18 CCC).

To meet the challenges resulting from the volatility of computer data, the list of measures does not only cover investigative powers (Art. 18 ff. CCC), but also provisional measures aimed at the preservation of electronic evidence (Art. 16, 17 CCC). The powers shall be subject to conditions and safeguards that balance the requirements of law enforcement with the the protection of human rights (Art. 15(1) CCC) and include both procedural (judicial or other independent supervision) and substantial (proportionality, limitation of certain measures to serious offences) requirements in accordance with the principles of the respective national criminal justice system (Art. 15(2) CCC).[15]

The provision on **production orders** distinguishes the disclosure of subscriber information and of any other computer data. According to Art. 18(1)(b) CCC, the competent law enforcement authority shall be empowered to order a service provider offering its services within national territory to submit **subscriber data** relating to such services and in that service provider's possession or control. Stretching the limits of enforcement jurisdiction, this treaty provision may be construed as extending to cross-border access to provider data because, unlike Art. 18(1)(a) CCC, it does not require the addressee of the production order to be legally or physically present on the territory of the investigating State Party.[16] Instead, jurisdiction is based on the connecting factor that the service provider is offering its services in the territory of the State Party. In this regard, the Cybercrime Convention Committee has proposed a twofold test: The service must be accessible from the territory of that State Party, and there must be a real and substantial link to the domestic population; relevant factors include the extent to which a provider interacts with and orients its activity toward local customers (for instance by local advertising), makes use of customer data in the course of its business activities or may otherwise considered established in the territory of the State Party.[17] Furthermore, the scope of Art. 18(1)(b) CCC is not limited to data in the service provider's physical possession, but also covers subscriber data under the service provider's control; in the latter case, the data may be stored at a remote storage facility provided by another company.[18] The Cybercrime Convention Committee has taken the view that the location of the requested data is not the determining factor for establishing jurisdiction and that, therefore, Art. 18(1)(b) CCC applies to subscriber information irrespective of where it is stored.[19] This wide interpretation, however, has not remained unchallenged.[20]

The wording of the general provision on the production of **computer data** (Art. 18(1)(a) CCC) is less far-reaching because the order can only be addressed to persons present within the territory of the

---

[15] Council of Europe, Explanatory report to the Cybercrime Convention https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b (31 August 2018), paras. 145 ff.

[16] Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 10, Production orders for subscriber information (Article 18 Budapest Convention), adopted by the T-CY following the 16th plenary by written procedure on 1 March 2017, T-CY (2015)16, para. 3.2.

[17] Cybercrime Convention Committee, T-CY Guidance Note # 10 (note 16), para. 3.6.

[18] Council of Europe, Explanatory report (note 15), para. 173.

[19] Cybercrime Convention Committee, T-CY Guidance Note # 10 (note 16), para. 3.5.

[20] P. de Hert, C. Parlar, and J. Saifert**, "**The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law", in *Computer Law & Security Review*, Vol. 34, 2018, Issue 2, pp. 327**–**336; see also D. Brodowski, "Transnational Organised Crime and Cybercrime", in P. Hauck and S. Peterke (ed.), *International Law and Transnational Organised Crime*, Oxford University Press, 2016, p. 352.

investigating State Party.[21] Nevertheless, the scope of this provision extends to any computer data that is in the addressee's "possession or control" and, thus, can be produced from within the ordering State's territory, irrespective of the location where the data is stored.[22]

2.1.2. International cooperation and cross-border access to provider data

In general, the cross-border collection of electronic evidence follows the traditional rules of international cooperation (MLA treaties and corresponding national legislation). Even though state parties shall cooperate to the widest extent possible (Art. 25(1) CCC), the international cooperation is subject to formal requirements (**request**) and **traditional refusal grounds** (double criminality, ordre public) apply (Art. 25(4) and (5) CCC; see also Art. 27(1), (4) CCC).

The general restrictions to international cooperation notwithstanding, the treaty provisions address the volatility of computer data and the resulting need for a swift and effective cross-border access to electronic evidence in a threefold manner:

First of all, MLA proceedings shall be accelerated by **expedited means of communication** (Art. 25(3) CCC), the designation of **central authorities** responsible for sending and answering MLA requests (Art. 27(2) CCC), direct contact between judicial authorities in urgent cases (Art. 27(9)(a) CCC) and the establishment of a 24/7 **network of contact points** permanently on duty (Art. 35 CCC).

Second, there are specific measures to address the challenges arising from the volatility of data. In this respect, the treaty provides for the **expedited preservation of stored computer data** (Art. 29 CCC). Like preservation orders in domestic proceedings (Art. 16 CCC, supra 2.1.1.), this provisional measure shall prevent the data from being deleted, altered or removed before a decision on a formal MLA request is taken and executed. Since the transfer of the secured evidence to the requesting state is subject to a final decision on the formal MLA request, the preservation shall not be subject to the full set of grounds for refusal, in particular double criminality shall be required in exceptional cases only (Art. 29(3), (4) CCC). Furthermore, if the requested state discovers that communication related to traffic data preserved under Art. 29 CCC has been transmitted by a service provider in third state, this traffic data shall be immediately disclosed to the requesting state to the extent necessary to initiate a request for expedited preservation to the third state (Art. 30 CCC).

Third, there are two exceptions from the general rule that cross-border access to stored computer data is subject to MLA proceedings (Art. 31 CCC). A state party may **unilaterally and directly access computer data stored abroad** if this data is publicly available (Art. 32(a) CCC) or if the data is accessed or received through a computer system in its territory, but located in another state party and if the accessing State Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system (Art. 32(b) CCC). The latter provision is considered to provide a legal basis for non-mandatory production requests to foreign service providers established in another State Party (see for the current practice supra 1.1.).[23] However, according to the

[21] Cybercrime Convention Committee, T-CY Guidance Note # 10 (note 16), para. 3.1.
[22] Cybercrime Convention Committee, T-CY Guidance Note # 10 (note 16), para. 3.1.; see also P. de Hert, C. Parlar and J. Saifert (note 20), p. 334.
[23] P. de Hert, C. Parlar and J. Saifert (note 20), p. 333 f.; B.J. Koops and M. Goodwin, "Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities International Law", in *Tilburg Law School Research Paper No. 5/2016*, 2014, p. 63, both referring to the explanatory report (note 16), para. 294.

Cybercrime Convention Committee, service providers are considered "unlikely" to to be able to consent validly to the disclosure of the data of its users because they only hold, but do not to own the data.[24]

The limited and controversial scope of these exceptions of the general MLA regime can hardly be reconciled with the extensive interpretation of Art. 18 CCC that promotes mandatory production orders in cross-border cases (supra 2.1.1.).[25] In particular, the scope of Art. 32(b) CCC is limited to "computer data located in another Party" and, thus, does not cover data stored in a third state.[26] Since a third state has not ratified the Convention and, thus, not given its prior consent to direct access to domestic data via non-mandatory production requests, such measures are considered to violate the territorial sovereignty of that state.[27]

To address the deficiencies and the ambiguities of the treaty framework, the Cybercrime Committee is preparing a **second additional protocol to the CCC**. The protocol shall provide for more effective MLA proceedings, rules allowing for direct cooperation with service providers in other jurisdictions, and a clearer framework and stronger safeguards, including data protection requirements, for existing mechanisms of cross-border access to computer data. The draft protocol shall be finalised by the end of 2019.[28]

2.2. Cross-border access to provider data under EU law: The European Investigation Order

Unlike the Cybercrime Convention, the EU has not yet adopted specific legislation on the cross-border access to electronic evidence, but created a general instrument for cross-border evidence-gathering: the European Investigation Order (EIO).[29] The EIO is based upon the **principle of mutual recognition** (Art. 67(3), 82(1) TFEU) and replaces the traditional framework of request-based MLA proceedings by a system of transnational judicial cooperation between the MS that issues the EIO (the issuing MS, formerly the requesting state) and the MS that recognises and executes the EIO (the executing MS, formerly the requested state). The implementation of the mutual recognition principle has significantly enhanced and facilitated cross-border cooperation within the EU by **standardised procedures** (forms, strict time-limits) and a **reduction of traditional grounds for refusal**.

The scope of the EIO covers any investigative measure aimed at gathering evidence, including electronic evidence (Art. 3 EIO Directive). An EIO may only be **issued** if it is in conformity with the proportionality principle and the investigative measure could have been ordered in a similar domestic case (Art. 6(1) EIO Directive). Furthermore, the EIO must be issued or validated by a **judicial authority** (judge, court, investigating judge, public prosecutor, Art. 2(c) EIO Directive).

---

[24] Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 3, Transborder access to data (Article 32), adopted by the 12th Plenary of the T-CY on 2–3 December 2014, T-CY (2013)7 E, p. 7 (3.6.).
[25] P. de Hert, C. Parlar, and J. Saifert (note 20), p. 332 f.
[26] Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 3 (note 24), 3.2.
[27] B.J. Koops and M. Goodwin (note 23), p. 63; U. Sieber, "Straftaten und Strafverfolgung im Internet: Gutachten C zum 69. Deutschen Juristentag", in Deutscher Juristentag (ed.), *Verhandlungen des 69. Deutschen Juristentages – München 2012*, Vol. 1 (Gutachten), C.H.Beck, 2012, p. 145; see also Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 3, 3.2., calling upon the State Parties to evaluate the legitimacy of such measures in the light of international law principles and considerations of international relations.
[28] Cybercrime Convention Committee (T-CY), Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, approved by the 17th Plenary of the T-CY on 8 June 2017, T-CY (2017)3, p. 3 f.
[29] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, O.J. L 130/1; see also Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, O.J. L 196/45, and Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, O.J. L 350/72.

The competent authority of the executing MS shall **recognise and execute the EIO** under the same conditions as if the investigative measure had been ordered by an authority of the executing MS (Art. 9(1) EIO Directive). In this regard, several traditional obstacles to MLA haven been abolished (such as the exceptions for political and fiscal offences). Nevertheless, the obligation to recognise and execute the EIO is still subject to a number of **grounds for refusal** (Art. 11(1) EIO Directive). In particular, the execution of an EIO may be refused if

- the investigative measure is prohibited by immunities or privileges under the law of the executing MS (Art. 11(1)(a) EIO Directive);
- the execution of the EIO would harm essential national security interests (Art. 11(1)(b) EIO Directive);
- the execution of the EIO would be contrary to the principle of *ne bis in idem* (Art. 11(1)(d) EIO Directive);
- the investigative measure is related to a criminal offence that has been committed outside the territory of the issuing State and wholly or partially on the territory of the executing State, and the conduct is not a criminal offence under the law of the executing State (Art. 11(1)(e) EIO Directive);
- the investigative measure is incompatible with the executing MS's obligation to respect fundamental rights according to Art. 6 TEU (Art. 11(1)(f) EIO Directive – European *ordre public*);
- the double criminality requirement is not met, unless the EIO has been issued with regard to a conduct that is covered by a list of 32 categories of offences (Art. 11(1)(g) and Annex D EIO Directive);
- the investigative measure is restricted under the law of the executing State to serious offences (catalogue offences or offences punishable by a certain threshold) and the offence to which the EIO refers does not meet this requirement (Art. 11(1)(h) EIO Directive).

In part (Art. 11(1)(a), Art. 11(1)(h) EIO Directive), the refusal grounds are based on the rationale that the EIO should not be executed if the **corresponding investigative measure** would not be **available in a similar domestic case**. The level of protection of fundamental rights shall not depend upon whether the evidence is to be used in domestic proceedings or in criminal proceedings conducted in another MS. Accordingly, if the EIO is issued to order a service provider to submit **traffic or content data** related to one of its users and the law of the executing MS provides that such a production order is restricted to specific catalogue offences, the execution of the EIO is subject to this condition, too.

As far as the MSs' national laws usually do not provide for such higher thresholds, the Directive determines a set of investigative measures that must be always available under the law of the executing MS (Art. 10(2) EIO Directive). Accordingly, they are not subject to the double criminality requirement and the limitation to serious offences (Art. 11(2) EIO Directive). This exemption applies to the identification of a person holding a subscription of a specified phone number or IP address (Art. 10(2)(e) EIO Directive) so that the execution of a corresponding EIO (**production of subscriber data**) must **not** be **subject to the double criminality requirement nor limited to serious offences**.

The EIO shall be executed with the **same celerity and priority as** for **a similar domestic case**, and urgent circumstances as indicated by the issuing authority shall be taken into account as much as possible (Art. 12(1), (2) EIO Directive). In any case, the executing authority shall take the decision on the recognition of the EIO within 30 days after receipt of the EIO and carry out the investigative measure within 90 days after the decision has been taken (Art. 12(3), (4) EIO Directive). In addition, the issuing authority may issue an EIO in order to prevent the destruction or removal of electronic evidence; the

executing authority shall carry out the **provisional measure** as soon as possible and, wherever practicable, **within 24 hours** of receipt of the EIO (Art. 32(1), (2) EIO Directive).

In sum, the EIO will considerably facilitate the gathering of electronic evidence within the EU by reducing traditional obstacles to cooperation and streamlining proceedings. As MSs have **implemented** the EIO Directive **most recently** and the corresponding national laws have entered into force in the period from May 2017 to August 2018,[30] it remains to be seen whether and to what extent the EIO will enhance cross-border access to provider data and resolve the problems linked to the previous framework of international cooperation. In any case, however, the executing MS still has to recognise and execute the EIO. In contrast to Art. 32 CCC, the EIO does not enable the issuing MS to directly access computer data or service providers in the executing MS. In contrast, extraterritorial operations like cross-border surveillance (Art. 40 CISA) are rather excluded from the scope of the EIO.[31]

[30] See the overview of the implementation of the EIO in the MSs provided by the European Judicial Network at: <https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120> (31 August 2018).
[31] Recital (9) EIO Directive (note 29).

3. THE COMMISSION'S PROPOSAL

KEY FINDINGS

- The Commission's proposal creates a framework for direct and mandatory cross-border cooperation between law enforcement authorities of the MS and service providers offering their services in the Union. According to the proposal, enforcement jurisdiction is established irrespective of the location where the requested data is stored. The material scope of the proposal is determined by precise definitions of the addressee (service provider). The definitions of the different categories of data build upon existing EU legislation and international treaty law, but leave room for ambiguities.

- The new cooperation instruments, the European Production Order (EPOC) and the European Preservation Order (EPOC-PR), entail an obligation of the addressee to produce or preserve the requested data, without prior recognition by the MS where the order shall be executed. Instead of the the executing MS, the issuing MS is assigned with the task to assess whether the conditions for the execution of the order are met. The conditions for issuing (and executing) the order are mainly defined by EU law and the law of the issuing MS.

- The service provider may refuse to execute the order in exceptional cases only (*de facto* impossibility, *force majeure*, violation of the European *ordre public*). If the service provider does not comply with its obligations, the MS where the service provider is addressed is obliged to enforce the order. The obstacles to enforcement are strictly limited to the conditions for issuing and executing the EPOC or EPOC-PR, and most refusal grounds established in other mutual recognition instruments do not apply (except for immunities and privileges under the law of the enforcing MS and national security interests).

- The proposal establishes a review procedure in the issuing state that shall resolve conflicting obligations of the service provider resulting from EU law (the EPOC) and the law of a third country prohibiting disclosure of the requested data, but it does not provide for a judicial remedy to challenge before the courts of the issuing MS the legality of the EPOC. In contrast, the person whose data was obtained by the EPOC shall have the right to effective remedies in the issuing MS.

- To ensure the functioning of the new cooperation instruments, the proposed directive provides for an obligation of service providers offering their services in the Union to designate a legal representative for receipt of, compliance with and enforcement of an EPOC or an EPOC-PR.

The new regime on direct access to electronic evidence as proposed by the Commission shall be based on two legislative measures, namely a regulation on European Production and Preservation Orders for electronic evidence in criminal proceedings (draft regulation) and a directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (draft directive). The regulation shall establish the European Production Order Certificate (EPOC) and the European Preservation Order Certificate (EPOC-PR) as new cooperation instruments implementing the principle of mutual recognition (3.1.) whereas the directive shall determine the addressee of these measures (3.2.).

3.1. The European Production Order and the European Preservation Order

3.1.1. Subject matter and scope

Subject matter and purpose of the proposed Regulation is the establishment of a new cooperation instrument whereby a law enforcement authority in one MS can order a service provider established or represented in another MS to produce or preserve electronic evidence. As mutual recognition instruments, the scope of the EPOC (Art. 2(1) draft regulation) and the EPOC-PR (Art. 2(2) draft regulation) is limited to cross-border cooperation whereas production and preservation orders addressed to domestic service providers are subject to the MSs' national laws (Art. 1(1) EPO draft regulation). The distinction between domestic and **cross-border access** is not any more based upon the place where the data is stored ("**regardless of the location of data**"), but upon the MS where the service provider is established or represented (Art. 1(1) draft regulation). Thereby, the Commission departs from the traditional rule of international cooperation that cross-border access to computer data requires consent of the state where the data is stored (Art. 25 ff. CCC, supra 2.1.2.).[32] **Jurisdiction** is not any more **linked** to the location of data, but **to the place where the addressee of the measure provides its services** (Art. 2(4) draft regulation); in this regard, however, the proposal can build upon Art. 18 CCC and its interpretation by the Cybercrime Convention Committee (supra 2.1.1.). According to the new approach (location of service), jurisdiction of the EU and its MSs can be established over service providers offering their services in the Union; this requirement is met if the service provider enables other persons in (at least) one MS to use its services and has a substantial connection to this MS (Art. 3(4) draft regulation). Thereby, the proposal avoids the difficulties in establishing the place where the data is actually stored ("loss of location"); the reasoning and the consequences of the new approach shall be analysed in section 4.

The scope by the new measures is furthermore determined by the potential addressees: An EPOC respectively EPOC-PR can only be issued against **service providers** offering one of the following services in the Union (Art. 2(3)(a)-(c) draft regulation):

- electronic communication services[33];
- information society services[34] for which the storing of data is a defining component of the service including social networks, online marketplaces and other hosting service providers);
- internet domain name and numbering services (IP address providers, domain name registries etc.).

Corresponding to the potential addressee of the order, the term "electronic evidence" only covers the data stored by or on behalf of a service provider (Art. 2(6) draft regulation). By issuing an EPOC or an EPOC-PR, the following categories of data can be obtained respectively preserved:

- **subscriber data**: the identity of a subscriber or customer (name, date of birth, address, billing or payment data, telephone or email) and the type of service and its duration, excluding passwords and other authentication means (Art. 2(7) draft regulation);

[32] Commission, Proposal for a Regulation (note 10), p. 13.
[33] The proposal refers to the definition according to Art. 2(4) of the Directive establishing the European Electronic Communications Code, see the Commission's proposal Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code, COM (2016) 590 final/2 of 12 October 2016, p. 124.
[34] Art. 1(1) Directive (EU) 2015/1535 of the European Parliament and the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), O.J. L 241/1.

- **access data**: data related to the commencement and termination of a user access session (date and time of the use, log-in to and log-off from the service, IP-address allocated to the user) which is strictly necessary for the sole purpose of identifying the user (Art. 2(8 draft regulation);
- **transactional data**: data related to the provision of a service offered by the service provider providing context or additional information about such service and generated or processed by an information system of the service provider such as destination and source of a message, location of the device, date, time and duration of the service, unless such data constitutes access data (Art. 2(9) draft regulation);
- **content data**: any other stored data in a digital format, in particular text, voice, videos, images (Art. 2(10) draft regulation).

The different categories of data reflect a varying level of interference with fundamental rights: Whereas disclosure of subscriber data establishes the identity of the user only, access to transactional data and content data reveals comprehensive information about the communication process and, therefore, should be subject to higher thresholds and safeguards.[35] The definitions widely correspond to the terminology in international treaty law and EU legislation (Directive 2002/58/EC on privacy and electronic communications[36]) that distinguishes subscriber data (Art. 18(3) CCC; see also Art. 10(2)(e) EIO Directive) from content data (Art. 21 CCC) and transactional data which has been referred to more specifically as traffic data (Art. 1(d) CCC, Art. 2(b) Directive 2002/58/EEC) and location data (Art. 2(c) Directive 2002/58/EEC).

Although the distinction between content, traffic and subscriber data is well-established throughout the Union, the definitions vary considerably from MS to MS. For instance, there is no common understanding on whether the definition of subscriber data covers dynamic IP addresses or whether or not content data should be related to communication.[37] The proposal builds upon the existing framework, but provides more precise definitions in order to establish a common framework for cross-border access to provider data. To that end, the proposal creates the new category of access data and avoids the ambiguities in the notion of subscriber data.[38] The disclosure of access data is strictly limited to the extent necessary for the identification of the user so that the distinction between access data and (other) transactional data appears justified.[39] Nevertheless, the concept significantly overlaps with the definition of transactional data and may give rise to legal uncertainty about the applicable threshold (Art. 5(3), (4) draft regulation; see infra 3.1.2.). On the other hand, the intrusiveness of the production order does not depend upon whether or not the data is related to communication so that the definition of content data is not limited to communication data[40], but extends to personal data processed and stored by information services (for instance cloud computing systems).[41] Again, the definitions of transactional data and content data ("any other stored data") are not clearly distinguished, either, but in this regard, one and the same threshold will apply (Art. 5(4) draft regulation).

[35] Commission, Proposal for a Regulation (note 10), p. 14; Cybercrime Convention Committee, T-CY Guidance Note # 10 (note 16), para. 2.2.
[36] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J. L 201/37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, O.J. L 337/11.
[37] Commission, Technical Document (note 7), p. 8
[38] See with regard to Art. 18(3) CCC: P. de Hert, C. Parlar and J. Saifert (note 20), p. 331.
[39] Commission, Proposal for a Regulation (note 10), p. 15.
[40] According to the Explanatory Report (note 15), content data (Art. 21 CCC) refers to the content of the communication and covers everything transmitted as part of the communication that is not traffic data (para. 229).
[41] Commission, Technical Document (note 7), p. 27.

The material scope of the proposal and the new instruments is limited to criminal proceedings during the pretrial and the trial phase (Art. 3(3) draft regulation); unlike the EIO, an EPOC or EPOC-PR must not be issued in proceedings on the imposition of an administrative fine (see Art. 4(b) EIO Directive). The new rules on the EPOC and the EPOC-PR do not affect other mutual recognition instruments so that it is up to the MSs' authorities to decide on whether to issue an EIO or an EPOC (Art. 23 draft regulation).

3.1.2. Issuing EPOCs and EPOC-PRs

Since the new cooperation instruments are based upon the principle of mutual recognition, the formal and substantial requirements for issuing an EPOC (or an EPOC-PR) have – at least partially – been developed from the corresponding rules on the EIO.

The EPOC and the EPOC-PR must be issued or validated by a **judicial authority** (judge, court, investigating judge; see supra 1.3. and Art. 2(c) EIO Directive); in contrast to an EPOC for transactional and content data (Art. 4(2) draft regulation), an EPOC for subscriber and access data and an EPOC-PR may be issued by a prosecutor, too (Art. 4(1), (3) draft regulation). The sensitivity of transactional and content data requires higher procedural safeguards (court authorisation). As a provisional measure, the EPOC-PR is not subject this requirement.

Like the EIO, an EPOC may only be issued if it is in conformity with the **proportionality** principle and if a similar measure (production order) would be available for the same criminal offence in a **comparable domestic case** (Art. 5(2) draft regulation; see supra 2.2. and Art. 6(1) EIO Directive).

Further requirements are related to the offence under investigation: Whereas an EPOC to produce **subscriber data and access data** may be issued for **any criminal offence** (Art. 5(3) draft regulation), access to **transactional and content data** is subject to a **higher threshold** (Art. 5(4) draft regulation) and an EPOC may only be issued

- for criminal offences punishable in the issuing MS by a custodial sentence of a maximum of at least 3 years;
- for harmonised offences committed by means of an information system (fraud and counterfeiting of non-cash means in payment[42], sexual abuse and sexual exploitation of children and child pornography[43], attacks against information systems[44]);
- terrorist offences[45].

At first sight, it seems doubtful whether such an additional requirement is necessary to protect fundamental rights because, as a matter of principle, the threshold under the law of the issuing MS should provide an adequate level of protection. Accordingly, the issuing of an EIO is not subject to such a condition. A closer look, however, reveals that the additional threshold results from a fundamental conceptual difference between the EIO and the EPOC: The execution of the EIO requires a prior decision of a competent authority of the executing MS whereas the EPOC is executed in another MS without prior recognition by that MS being necessary. As a consequence, the "executing" MS (the MS where the

[42] Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, O.J. L 149/1.
[43] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, O.J. L 335/1.
[44] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, O.J. L 218/8.
[45] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, O.J. L 88/6.

EPOC is executed) does not assess whether the conditions for execution are met, and the individual is deprived of a control mechanism aimed at the protection of his/her fundamental rights.

The Commission's proposal addresses these concerns by **shifting tasks and competences from the executing MS to the issuing MS** so that it is for the issuing state to assess whether the conditions for the execution of the EPOC are met. From this perspective, the distinction between subscriber data and access data on the one hand, and transactional data and content data on the other is reflected in the corresponding refusal grounds for the EIO.

As a matter of principle, the EIO Directive has maintained traditional rules of cross-border cooperation such as the double criminality requirement and the analogous application of thresholds for particularly intrusive investigative measures (Art. 11(1)(g) and (h) EIO Directive). Nevertheless, these refusal grounds have been waived for the collection of subscriber data (Art. 10(2), Art. 11(2) EIO Directive) because this kind of data was considered less sensitive, and its collection and transfer to the issuing MS should therefore no longer be subject to the double criminality requirement nor a specific threshold. In contrast, these requirements are still relevant for accessing transactional data and content data (Art. 11 (1)(g) and (h) EIO Directive). In its core, the threshold as defined in Art. 5(4) draft regulation incorporates the exception from the double criminality requirement (Art. 11(1)(g) EIO Directive). There are, however, major differences in the level of protection:

- The conditions for the exception from the double criminality requirement (minimum maximum penalty and offence covered by the list of 32 categories of offences) are not cumulative (Art. 11(1)(g) EIO Directive), but alternative (Art. 5(4)(a), Art. 5(4)(b) and (c) draft regulation). Even though the offences do not refer to the full list of 32 categories of offences, the alternative reference to both criteria allows for access to transactional and content data to a significant extent without regard to the double criminality requirement.
- The threshold under the law of the executing MS (Art. 11(1)(h) EIO Directive) is not mentioned at all; as a consequence, the execution of the EPOC may bypass a higher level of protection under the law of the MS where the order shall be executed.

In contrast, other **refusal grounds** referring to the MS where the EPOC shall be executed (privileges and immunities, national security interest, see Art. 11(1)(a) and (b) EIO Directive) are **re-formulated as obstacles to the issuing of an EPOC**. In this regard, the wording is not clear whether the scope of these restrictions is limited to transactional and content data only (Art. 5(7)1 draft regulation) or extends to access data (Art. 5(7)2 draft regulation). In any case, the exceptions do not apply to subscriber data as disclosure of this data is unlikely to affect privileges, immunities or national security interests.

As far as the issuing of an EPOC is concerned, the draft regulation does not mention any other refusal grounds for the EIO (for instance the principle of *ne bis in idem* or the European *ordre public*, Art. 11(1)(d) and (f) EIO Directive). A likely reason is that the issuing authority must anyway comply with fundamental rights enshrined in Art. 6 TEU which is also reflected in the general conditions for issuing an EPOC, the principle of proportionality in particular (Art. 5(2) draft regulation; see also Art. 1(2) draft regulation). Furthermore, the issuing authority usually does not have the information necessary to assess whether a ground for not issuing the EPOC is given (for instance a final judgment in the executing MS). This lack of information is also reflected in the wording of Art. 5(7) draft regulation ("If the issuing authority has reasons to believe …"). It would contradict the very objective of the

Commission's proposal to burden the issuing authority with the obligation to assess whether the execution of the EPOC is in conformity with the law of another MS (see for the double criminality requirement and the territoriality principle: Art. 11(1)(e) EIO Directive). In this regard, however, the Commission's approach does not appear consistent: If there are reasons to believe that the requested data is protected by immunities and privileges under foreign law, the issuing authority must seek clarification before issuing the EPOC and, if necessary, contact the MS concerned (Art. 5(7) draft regulation). In any case, there is a general tendency not to incorporate the refusal grounds provided for the EIO and, thereby, to facilitate and accelerate cross-border access to provider data. In section 5, it will be examined whether or not this concept provides for an adequate protection of fundamental rights (see infra 5.1.).

As far as the issuing an EPOC-PR is concerned, there are only few substantial requirements because the **preservation** is an urgent and **provisional measure** and the issuing authority has to assess the conditions for the production of the preserved data before issuing an EPOC to that end. For this reason, the competent authority may issue an EPOC-PR if the preservation is necessary and proportionate to prevent the removal, deletion or alteration of data in view of a subsequent production of this data (Art. 6(2)1 draft regulation). The measure applies to any criminal offence (Art. 6(2)2 draft regulation).

The EPOC and the EPOC-PR shall be addressed directly to a legal representative designated by the service provider (Art. 7(1) draft regulation; see infra 3.2.). If a designated legal representative does not exist or does not comply with its obligations, the order may be addressed to any establishment of the service provider in the Union (Art. 7(2)-(4) draft regulation). For issuing EPOCs and EPOC-PRs, the competent authority shall use standard forms (Annexes I and II draft regulation) in order to provide the necessary information in a standardised format, to minimise sources of error and to reduce costs for translation.[46]

3.1.3. Execution of EPOCs and EPOC-PRs

The EPOC and the EPOC-PR are transnationally binding decisions that entail the obligation for the service provider to produce respectively preserve the requested data (Art. 9, 10 draft regulation). The execution does **not require prior recognition** by the MS where the EPOC or the EPOC-PR is executed. By avoiding time-consuming MLA proceedings (respectively proceedings on the recognition and execution of an EIO), the proposal shall ensure quick and effective cross-border access to provider data: The data must be transmitted within 10 days, in urgent cases within 6 hours (Art. 9(1) and (2) draft regulation).

There are only few **exceptions** from the obligation to execute the EPOC or the EPOC-PR. If the order is incomplete or contains manifest errors or if the addressee cannot comply with its obligation because of *force majeure* or *de facto* impossibility, in particular because the person whose data is sought is not its customer, the addressee shall contact the issuing authority without undue delay (Art. 9(3), (4) and Art. 10(4), (5) draft regulation).

In addition to these inherent limitations to the obligation of the addressee, another exception refers to the **European *ordre public***. According to Art. 9(5) draft regulation, if the addressee considers that the EPOC cannot be executed because it manifestly violates fundamental rights or it is manifestly abusive,

[46] Commission, Proposal for a Regulation (note 10), p. 18.

it shall contact both the issuing authority and the competent enforcement authority in the MS of the addressee. Due to the high threshold ("manifestly"), this provision will apply to exceptional cases only, for instance to an order requesting the production of content data pertaining to undefined group of people in a geographical area or with no link to concrete criminal proceedings).[47] In cross-border cooperation, the *ordre public* clause is usually applied by the competent authority in the executing (requested) MS (Art. 11(1)(f) EIO Directive). In section 5, it shall be further examined service providers can ensure an equivalent protection of fundamental rights (see infra section 5.1.2.).

The **limited number of grounds for non-execution** suggests that the addressee must not refuse to produce (or preserve) the requested data for other reasons, for instance if if the formal and substantial requirements for issuing an EPOC or an EPOC-PR are not met (supra 3.1.2.). This issue shall be subject to further discussion in the section on enforcement (infra 3.1.4) and judicial remedies (infra 3.1.5.).

3.1.4. Sanctions and Enforcement of EPOCs and EPOC-PRs

If the service provider does not produce or preserve the requested data, the EPOC respectively EPOC-PR shall be enforced by the competent MS where the service provider is established or represented (the enforcing MS). To that end, the draft regulation requires MS to provide for sanctions (Art. 13) and to ensure enforcement (Art. 14).

The enforcement mechanism follows the general concept of mutual recognition instruments such as the EIO (Arts. 9 ff. EIO Directive), the only difference being that the executing authority is transformed to the enforcing authority: EPOCs and EPOC-PRs directly entail binding obligations upon service providers so that a formal recognition decision is not required for execution (supra 2.1.3.), but only for enforcement (Art. 14(2) draft regulation).

The procedure for enforcement consists of three phases (recognition, confirmation of enforceability, enforcement). In the first phase, the enforcing authority recognises the EPOC or EPOC for the purpose of enforcement unless it considers that one of the **grounds for refusal** applies. These grounds correspond to:

- the formal (judicial authorisation) and substantial (threshold) requirements for and the general restrictions (immunities and privileges, national security) to issuing an EPOC or an EPOC-PR (Art. 14(2), (4)(a), (b), (5)(a) draft regulation);
- the grounds for non-execution (*force majeure*, impossibility, European *ordre public*) of an EPOC or an EPOC-PR (Art. 14(4)(c), (d), (f), (5)(b), (c), (e) draft regulation);
- the limitations of the scope of the regulation to specific services (Art. 14(4)(e), (5)(d) draft regulation).

If the enforcing authority recognises the order, it shall formally require the addressee to comply with its obligation and provide the addressee with the opportunity to oppose the enforcement by invoking one of the refusal grounds (Art. 14(3) draft regulation). If the addressee does not oppose the enforcement or its objections are unfounded, the enforcing authority confirms the enforceability of the order and notifies the addressee and the issuing authority of its decision (Art. 14(6), (8) draft regulation). Finally, if the service provider still fails to comply with its obligation to produce or preserve the requested data, the enforcing authority shall impose a pecuniary sanction; the addressee must be

[47] Commission, Proposal for a Regulation (note 10), p. 21.

provided with an effective judicial remedy against the sanctioning decision (Art. 14(10) draft regulation).

The three-stage enforcement procedure provides for procedural safeguards that are essential for the protection of the rights of service provider to which the EPOC or the EPOC-PR has been addressed, notably the right to be heard and to the right to an effective judicial remedy against the sanctioning decision.

The effectiveness of judicial protection in the enforcing MS, however, is compromised by the **limited number of refusal grounds**. The draft regulation provides for a rather far-reaching obligation of the enforcing authority to recognise and enforce of an EPOC or EPOC-PR. The obstacles to enforcement are strictly limited to the conditions for issuing and executing the order so that several grounds for refusal in other mutual recognition instruments do not apply and the individual is deprived of the protection under the law of the executing respectively enforcing MS (double criminality requirement, restrictions to serious offences, supra 3.1.2.). In this regard, protection of immunities and privileges according to the law of the enforcing MS is rather the exception than the rule. Furthermore, recourse to the European *ordre public* is limited to manifest violations of fundamental rights that are apparent from the sole information contained in the order (Art. 14(4)(f), (5)(e) draft regulation; see supra 3.1.3.).

On the other hand, the grounds for refusal do not fully correspond to the conditions for issuing an EPOC or EPOC-PR since the enforcing authority does not assess the legality of the EPOC under the law of the issuing MS, in particular whether the production order is proportionate and would be available in a comparable domestic case (Art. 5(2) draft regulation). As a consequence, the service provider might be forced to execute an EPOC that has not been adopted in accordance with the law of the issuing MS. This issue will be subject to closer examination in section 5 (see infra 5.1.1.).

In the framework of international cooperation, this problem is usually addressed by legal remedies available in the issuing MS (Art. 14(2) EIO Directive). In this regard, the proposal provides for a review procedure in the issuing MS, but the scope of this procedure is limited to conflicts with the laws of a third country (Art. 15, 16 draft regulation). There might be a need for further judicial remedies in the issuing MS (see infra 3.1.5. and 5.1.3.).

3.1.5. Judicial remedies

The obligations arising from EPOCs and EPOC-PRs affect the legal position of the service provider and the person whose data shall be transmitted. Accordingly, the proposal provides for legal remedies in the issuing MS enabling the service provider and the individual person to challenge the order.

As far as remedies for service providers are concerned, the proposal focuses on the situation where the **service provider's obligation** to produce the requested data **conflicts with its obligations under the law of a third country** (Art. 15, 16 draft regulation). Such a situation may arise where a service provider is headquartered in a third country whose law prohibits the disclosure of the requested data. In this case, compliance with the EPOC may carry the risk of criminal and civil liability under the law of the third state. To resolve this conflict, the proposal establishes a review procedure in the issuing MS. Taking the obligations under the law of a third country into consideration, the **review mechanism** is also important for the protection of individual rights of the user and the sovereign interests of the third state.

If the service provider considers that the law of a third country prohibits the disclosure of the requested data it shall file a reasoned objection to the EPOC (Art. 15(1), (2)1; Art. 16(1), (2)1 draft regulation). If the issuing authority considers the objection to be unfounded, it shall request a review of the competent court (Art. 15(3)2, Art. 16(3)2 draft regulation). The court shall lift the EPOC if the following conditions are met:

- The law of the third country applies to the case and prohibits disclosure of the data concerned. The court's assessment must be based on the specific circumstances of the case rather than the mere fact that similar investigative measures are not available under the law of the third country or the only circumstance that the data is stored in this country (Art. 15(2)2, (3)4); Art. 16(2)2, (4) draft regulation).
- If the conflicting obligation under the law of a third country is aimed at the protection of fundamental rights or fundamental interests of the third country (national security), the court shall also consider whether the third country law manifestly seeks to protect other interests or to shield illegal activities from criminal investigations (Art. 15(4) draft regulation). If the court establishes a relevant conflict of obligations it shall contact the central authority of the third state. If the central authority objects to the execution of the EPOC, the court shall lift the order; if the court does not receive such an objection within 15 days (or 30 days if the deadline is extended), it shall upheld the EPOC (Art. 15(5), (6) draft regulation).
- If the conflicting obligation under the law of a third country is not aimed at the protection of fundamental rights or fundamental interests of the third state, the decision of the court to lift or upheld the EPOC shall be based on a balancing of interests, namely the interests protected by the third country law, the interests of the issuing MS and the interests of the service provider; in particular, the jurisdictional links of the case under investigation and the service provider to the third state and the issuing MS shall be taken into consideration (Art. 16(5) draft regulation).

The review procedure does not only relieve the service provider from a conflict of obligations under EU law and the law of a third state, but also maintains higher data protection standards in third countries (Art. 15 draft regulation).[48] On the other hand, to ensure the proper functioning of the new instrument, the establishment of conflicting obligations is subject to strict requirements and confirmation by the central authority of the third state. The mechanism, thus, appears to be an appropriate and well-balanced solution.

However, the remedy is limited to a specific situation (conflicting obligations) and does not provide for a general procedural framework of judicial review in the issuing MS. The **general provision on judicial remedies** only applies to the person whose data has been obtained via an EPOC (Art. 17 draft regulation).[49] According to the proposal, the remedies of the service provider are limited to the enforcement procedure (Art. 14 draft regulation, supra 2.1.4) and the review procedure for conflicting obligations (Art. 15, 16 draft regulation).[50] Thus, the proposal apparently does not provide the service provider with a legal remedy to challenge the legality of the EPOC or the EPOC-PR in the issuing MS (for further discussion see infra 5.1.3.).

[48] Commission, Proposal for a Regulation (note 10), p. 21.
[49] Commission, Proposal for a Regulation (note 10), p. 21: "Other grounds [than the refusal grounds mentioned in Art. 14, M.B.] can only be invoked by the person whose data is being sought, in the framework of their own legal remedies in the issuing State …".
[50] Commission, Proposal for a Regulation (note 10), p. 23: "Unlike what is provided for service providers, the Regulation does not limit the possible grounds for all these persons to challenge the legality of the Order …".

Unlike the service provider, the **individual person whose data was obtained** shall have the right to an **effective remedy** against the EPOC that includes the right to challenge the legality of the order according to the law of the issuing MS (Art. 17(1), (3) draft regulation). The right to an effective remedy applies to suspects and accused persons as well as to third persons whose data has been transmitted (Art. 17(1), (2) draft regulation). The scope of the remedy is limited to EPOCs because an EPOC-PR does not allow for the disclosure, but only for the (temporary) preservation of personal data: If the EPOC-PR is not followed by a subsequent EPOC, the preservation will cease (Art. 10(1) draft regulation) so that there is no need for a legal remedy.[51] The issuing state must take the appropriate measures to ensure that the person concerned is informed of the execution of the EPOC (Art. 17(2), (3) draft regulation) and the available remedies and that these remedies can be exercised effectively (Art. 17(4) draft regulation). In this respect, however, the proposal leaves room for ambiguities as the provision on confidentiality of the investigation suggests that the issuing authority's obligation to provide information about available remedies does not apply where the service provider has not been requested to refrain from informing the person concerned about the data production (Art. 11(2), (3) draft regulation).

As far as the issuing MS is concerned, the proposal provides an adequate framework for effective judicial protection. Nevertheless, it does not foresee any judicial remedies in the enforcing MS. As a matter of fact, if the EPOC is executed without an enforcement procedure being necessary, there is no recognition decision of the enforcing authority that can be subject to judicial review. Even if an enforcement decision is taken, the assessment of the enforcing authority does not extend to the legality of the order under the law of the issuing MS. Thus, the **concentration of judicial review in the issuing MS** is a consequence of the Commission's concept to create a transnationally binding production order and to abolish refusal grounds deriving from the law of the MS where the EPROC is executed (supra 3.1.2.). Accordingly, the courts of the issuing MS are "best placed" to review the legality of the EPOC under their own law.[52]

This latter reasoning does not apply as far as the issuing authority must examine whether the requested transactional or content data is protected by immunities or privileges under the law of the MS where the service provider is addressed or by provisions related to fundamental interests of that MS (Art. 5(7) draft regulation). This obligation notwithstanding, there may be cases where such data is transmitted because neither the issuing authority nor the service provider realises that the requested data enjoys special protection. In this case, the proposal seeks to maintain this protection during criminal proceedings in the issuing state by establishing an obligation of the trial court, when assessing the relevance and the admissibility of evidence, to take these grounds for protection into account in the same way as if they were provided for under domestic law (Art. 18 draft regulation). Thus, depending on the issuing MS's law on the exclusion of evidence, the transmitted data might not be used as evidence because it is protected by immunities or privileges under the law of the MS where the service provider was addressed. Like a similar rule for the EIO (Art. 14(7) EIO Directive), this provision seeks to ensure that the level of protection granted by the enforcing MS is maintained. Still, the protection is limited to privileges and immunities and does not apply to other conditions and safeguards under the law of the enforcing MS (for instance a restriction of the measure to serious offences, see infra 5.1.1. and 5.1.3.).

[51] Commission, Proposal for a Regulation (note 10), p. 22.
[52] Commission, Proposal for a Regulation (note 10), p. 23.

3.2. The legal representative as (potential) addressee of the new instruments

As has been mentioned above, the EPOC and the EPOC-PR shall be addressed to a legal representative designated by the service provider (Art. 7(1) draft regulation; see supra 3.1.2.). The directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (draft directive) shall **ensure** that such a **designation** has taken place so that the **legal representative can produce and preserve the requested data** even if it is held by a service provider not established in the Union. In addition, the proposal shall create a level playing field for service providers offering their services in the Union and, thereby, contribute to a better functioning of the internal market.[53]

Subject matter and scope of the directive widely correspond to the draft regulation on the EPOC and the EPOC-PR (supra 3.1.1.). The proposed directive shall apply to service providers offering their services in the Union (Art. 1(4)1, Art. 2(2), (3) draft directive; see supra 3.1.1.). The directive is not applicable if a service provider is established and offers services in the territory of a single MS (Art. 1(4)2 draft directive). In this case, production and preservation orders can be addressed directly to the establishment of the service provider.[54] The same applies to any other domestic order because the proposal does not prejudice the investigative powers of the MSs' competent authorities to address service providers established on their territory (Art. 1(3) draft directive).

Key element of the proposal is the obligation of a service provider to designate a **legal representative for receipt of, compliance with and enforcement of decisions and orders** issued by competent authorities of MSs **for the purpose of gathering evidence in criminal proceedings**. Thus, the obligations of the legal representative are not limited to EPOCs and EPOC-PRs, but also apply to orders and decisions in domestic criminal proceedings (Art. 1(1), Art. 3(5) draft directive). The legal representative shall reside or be established in one of the MSs where the service provider is established or offers his services (Art. 3(1), (2) draft directive). Furthermore, the legal representative must not be appointed in a MS where the new cooperation instruments do not apply (Art. 3(3) draft directive); this provision refers to the MSs that have opted out of (or not opted in) the judicial cooperation in criminal matters (Denmark, Ireland and the United Kingdom).[55] Apart from these requirements, the **service providers are free to choose in which MS they appoint their legal representative**, and MSs may not restrict this choice by imposing an obligation to designate a legal representative for the sole reason that the services are offered in their territory (see also Art. 1(2) draft directive).[56] Thereby, the directive follows the reasoning of the **country of origin principle** according to which MSs may not restrict the freedom to provide services from another MS (Art. 3(2) e-commerce Directive[57]).[58] The underlying rationale is to enable the service provider to designate one single legal representative for any production and preservation order issued by a competent authority of a MS.

This exclusive responsibility of the legal representative notwithstanding, the competent authority may address any other establishment of the service provider if the establishment lies within national territory (domestic access, Art. 1(3) draft directive) or if the service provider (or its legal representative)

[53] Commission, Proposal for a Directive (note 11), p. 3, 4.
[54] Commission, Proposal for a Directive (note 11), p. 7.
[55] Commission, Proposal for a Directive (note 11), p. 10. The Republic of Ireland, however, has already expressed its wish to take part in the adoption and the application of the new instruments, Council-Document 11375/18 of 24 July 2018, p. 2.
[56] Commission, Proposal for a Directive (note 11), p. 7, 9.
[57] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, O.J. L 178/1.
[58] See also Commission, Proposal for a Directive (note 11), p. 3.

has not complied with its obligations (Art. 7(2)-(4) draft regulation, supra 3.1.2.). Furthermore, the service provider shall be free to designate additional legal representatives and to decentralise the performance of the cooperation obligations established by the proposal (Art. 3(4) draft directive).

The service provider must provide its legal representative with the **necessary powers and resources to comply with production and preservation orders** (Art. 3(7) draft directive). The lack of internal procedures between the service provider and its representative cannot justify non-compliance (Art. 3(8) draft directive). The MS shall lay down sanctions applicable to service providers infringing their obligation to designate a legal representative (Art. 5(1) draft directive). The sanctions for non-compliance with the order are laid down by national law (supra 3.1.4.).

4. ENFORCEMENT JURISDICTION AND TERRITORIAL SOVEREIGNTY

KEY FINDINGS

- Extending enforcement jurisdiction to service providers and/or data located in a non-Member State, the Commission's proposal is driven by the volatility of computer data and supported by the theoretical concept of unterritoriality of data. In the light of corresponding developments in international treaty law and national legislation, enforcement jurisdiction solely based upon the place where the service provider offers its services cannot be considered to be a violation of state sovereignty under international law. Nevertheless, a unilateral extension of enforcement jurisdiction may compromise the functioning of international cooperation in criminal matters and foster conflicting obligations of service providers.

- The establishment of enforcement jurisdiction irrespective of the location of data may create legal uncertainty about the states competent to access user data. The connecting factor should be strictly construed in order to enable the user to foresee which enforcement regime(s) will apply to his/her data.

- The creation of a transnationally binding order may interfere with the sovereignty of MS in whose territory the order shall be executed (the enforcing MS). There are doubts whether Art. 82(1) TFEU provides a sufficient legal basis for the establishment of direct cross-border cooperation between law enforcement authorities and service providers. In any case, the sovereignty of the enforcing MS and its responsibility to protect the rights of its citizens call for an additional mechanism involving that MS (for instance by notification and ex-post consent).

The new regime of unilateral direct cross-border access to provider data reaches beyond the territorial boundaries of the issuing MS, and thereby affects the sovereignty of other states. The extraterritorial dimension of the Commission's proposal is twofold: On the one hand, the proposal may interfere with the territorial sovereignty of a non-Member State by extending enforcement jurisdiction of the issuing MS to service providers and data located in that state (4.1.). On the other hand, the new cooperation instruments will create a transnationally binding obligation of its addressee within the Union that fundamentally differs from the current legal framework of international cooperation in the AFSJ and that may interfere with the traditional concept of territorial sovereignty (4.2.).

4.1. Relations to non-Member States

Claiming jurisdiction beyond the territories of its MSs, the Union may interfere with the sovereignty of the third state where the service provider is established or where the requested data is stored (4.1.1.). Even if a violation of principles of international law cannot be established, the unilateral approach of the Commission's proposal may have a negative impact on legal certainty (4.1.2.) and international relations (4.1.3.).

4.1.1. International law and state practice

Since the judgment of the **Permanent Court of Justice** in the **Lotus-case**, it has been well- established under international law that a **state must not exercise its power within the territory of another**

state.[59] Coercive measures in the framework of criminal investigations (arrest, search, seizure) require the consent of the state on whose territory these measures are enforced; otherwise these measures violate the territorial sovereignty of that state.[60] Instead, the investigating state is held to act within the framework of international cooperation in criminal matters and not to bypass its requirements by exercising extraterritorial powers.

The legal situation becomes more complex if **coercive measures** are not carried out, but **produce their effect on the territory of another state**. The prevalent use of subpoena orders illustrates that the US are less concerned about territorial sovereignty with regard to such measures. A **subpoena order** requires a person who is within its jurisdiction to produce evidence that is located in another state. The international framework of mutual legal assistance is not considered to be exclusive, nor is the use of subpoenas held to be in breach with international law because subpoenas are based upon extraterritorial jurisdiction to prescribe which is subject to less strict requirements under international law and jurisdiction to enforce is exercised within domestic territory only.[61] In contrast, the US legislation on the obligation of service providers to disclose user data was interpreted rather restrictively: In the Microsoft-Ireland-case, an US court held that a warrant against the service provider to seize content data on its customer's communications stored abroad constituted an unlawful extraterritorial application of the US Stored Communications Act. The court explicitly distinguished between subpoenas and warrants and argued that the strict interpretation of US legislation also served the interest of comity and the international framework of mutual legal assistance.[62] In the aftermath of this decision, however, the US Cloud Act amended the legal framework and clarified that service providers were obliged to provide the requested data regardless of whether the data is located within or outside of the United States.[63] After the US government obtained a new warrant that expressly covered the information stored abroad, the case became moot and was dismissed by the US Supreme Court.[64]

Cross-border gathering of evidence by production orders, however, has remained a controversial issue, and several states (among others France[65] and Germany[66]) have **traditionally objected to coercive measures having extraterritorial effect** because such orders or warrants were considered to violate the territorial sovereignty of the state in which the required evidence (documents, records etc.) is located, in particular if the submission of the relevant documents is prohibited under the *lex loci*.[67] According to this point of view, cross-border access to electronic data must be subject to the same restrictions, and the obligation of service providers to produce data stored abroad is considered to

[59] Permanent Court of International Justice, Judgment of 7 September 1927, Ser. A no. 10, p. 18–19.
[60] See also Art. 4(2) of the UN Convention against Transnational Organized Crime of 15 November 2000, United Nations Treaty Series, vol. 2225, p. 209.
[61] US Court of Appeals, Ninth Circuit, Order of 3 June 1994, Opinion of 7 November 1994, In re Grandjury Proceedings, Marsoner v. U.S. 40 F 3d 959 (9th cir. 1994) 965–966; see also for the pretrial discovery in civil proceedings: US Supreme Court, 15 June 1987, . Societe Nationale Industrielle Aerospatiale et al. v. United States District Court for the Southern District of Iowa, 482 U.S. 522 (1987).
[62] US Court of Appeals, Second Circuit, 9 December 2016, In the matter of a Warrant to Search a Certain E-mail Account Microsoft v. US 829 F.3d 197 (2nd Cir. 2016) 214–216, 221.
[63] § 103(a)(1) Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 23 March 2018.
[64] US Supreme Court, 17 April 2018, United States v. Microsoft Corp., 138 S. Ct. 1186, 1188 (2018).
[65] Brief for France as Amicus Curiae Judicial and Similar Proceedings: United States: Supreme Court Proceedings in Societe Nationale Industrielle Aerospatiale et al. v. United States District Court for the Southern District of Iowa, International Legal Materials 25 (1986), p. 1519, 1524, 1528.
[66] Brief for Federal Republic of Germany as Amicus Curiae Judicial and Similar Proceedings: United States: Supreme Court Proceedings in Societe Nationale Industrielle Aerospatiale et al. v. United States District Court for the Southern District of Iowa, International Legal Materials 25 (1986), p. 1539, 1546.
[67] See further references to state practice provided by M. Schaub, „Zur völkerrechtlichen Zulässigkeit des amerikanischen Editionsbefehls an die UBS im Streit um die Kundendaten", in *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, Vol. 71, 2011, pp. 807, 811 ff.

violate the sovereignty of the foreign state in which the data is stored.[68] This understanding is also mirrored in Art. 32(b) CCC where cross-border access to computer data is limited to data located in another State Party (supra 2.1.2.).[69]

It cannot be denied, however, that recent developments have moved away from data storage as the determining factor for establishing enforcement jurisdiction. This tendency is clearly reflected in the **Cybercrime Convention Committee's guidance note** on production orders (supra 2.1.1.) and the laws of MSs providing for cross-border access to computer data.[70] According to Belgian law, any provider of electronic communication services active in Belgium must, upon request of the public prosecutor, disclose identification data irrespective of whether or or not the data is stored within Belgian territory. The **Belgian Court of Cassation** held that criminal sanctions for a failure to comply with such a request does not violate international law because the sanction and the request refer to a conduct within Belgian territory and, therefore, do not affect the territorial sovereignty of another state.[71] Similarly, the **Irish Supreme Court** found that an Irish court, if certain conditions were met, had the power to order the production of documents from an Irish company even if the required objects were located on foreign territory.[72] Most recently, the **German** legislator has adopted the **Network Enforcement Act** ("Netzwerkdurchsetzungsgesetz") that establishes a mandatory cooperation regime for service providers whose services can be accessed from German territory.[73] As the scope of the cooperation regime covers both domestic and foreign service providers, the obligation to produce provider data applies irrespective of the place where the data is stored.

Obviously, these recent developments have resulted from the need to address the challenges posed by modern information and communication technology and the volatility of computer data. If data is moved between servers in varying locations or - as in cloud computing systems - even scattered over several jurisdictions, reference to that place where the data is actually stored or processed becomes more or less arbitrary. According to some scholars, **computer data** has become an **"unterritorial"** medium for which the concept of territoriality no longer fits.[74] This approach is mirrored in the problems encountered by law enforcement authorities seeking to establish the location of data moving between several jurisdictions ("loss of location"). Since the storage location often depends on business considerations (cost efficiency), it may even be unknown to the user who does not care about the jurisdiction in which his/her data are processed and stored.[75]

The assumption that computer data is unterritorial is based upon an appealing, but rather far-reaching concept. If the choice of the storage location has been based on a deliberate decision of the user, it cannot be denied right from the outset that the user may legitimately expect his/her data being

[68] R.J. Currie, "Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the *Microsoft Ireland* Case the «Next Frontier»?", in *The Canadian Yearbook of International Law 2016*, Vol. 54, Cambridge University Press, pp. 63, 93; see also U. Sieber (note 27), p. 147.
[69] Cybercrime Convention Committee (T-CY), Report of the Transborder Group (note 5), p. 27.
[70] Cybercrime Convention Committee (T-CY), Report of the Transborder Group, (note 5), p. 32 ff. (Belgium, Portugal); R.J. Currie (note 68), p. 81–82 (United Kingdom, Ireland); A. Klip, "Section IV – International Criminal Law. Information Society and Penal Law – General Report", in *International Review of Penal Law*, Vol. 85, 2014, pp. 381, 406, 409 f. (Belgium, Denmark, France) and for the contrary view 406 f. (Germany, Italy, the Netherlands).
[71] Hof van Cassatie (note 2).
[72] Supreme Court of Ireland, 25 January 2013, Walsh v. National Irish Bank, Appeal No. 267/2007, [2013] 1 ESC 2, para. 9.3. ff.
[73] §§ 1, 5 Network Enforcement Act of 1 September 2017, Bundesgesetzblatt 2017, part I, p. 3352.
[74] J. Daskal, "The Un-Territoriality of Data", in *Yale Law Journal*, Vol. 125, 2015–2016, p. 326 ff.; P.S. Bermann, "Legal Jurisdiction and the Deterritorialization of Data", in *Vanderbilt Law Review*, Vol. 71, 2018, p. 11 ff.
[75] C. Warken, "Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus – Teil 1", in *Neue Zeitschrift für Wirtschaftsstrafrecht*, 2017, p. 289, 295.

protected by the law of the state where the data is stored.[76] Even though computer data, thus, cannot be *per se* considered "unterritorial", territorial jurisdiction is not necessarily linked to the location of the requested data. Instead, a **territorial link** can also be **based on other connecting factors** (such as the place where the service provider is established or where its services are offered).[77] Therefore, the concept of deterritorialisation must not be understood to abolish territorial jurisdiction as such, thereby allowing for unlimited cross-border access to computer data in cyberspace, but to replace (or supplement) the location of data by other grounds for enforcement jurisdiction.

The assessment whether the Commission's proposal is in line with international law cannot ignore the aforementioned tendencies in international treaty law and national legislation. According to the Commission's proposal, enforcement jurisdiction is based on a connecting factor that has been referred to in international treaty law and national legislation (the place where the service provider offers its services, Art. 2(4) draft regulation, see supra 3.1.1.). Furthermore, the sovereignty of the third state concerned (for instance the state in which the service provider is headquartered) is taken into account by the provisions on conflicting obligations under the *lex loci* (Art. 15, 16 draft regulation, see supra 3.1.5.).

All things considered, the current state of customary international law hardly allows for the conclusion that the cooperation regime proposed by the Commission would violate international law because its scope were not limited to data stored within the Union.

4.1.2. Deterritorialisation of data and legal certainty

The deterritorialisation of data and the elimination of storage location as a connecting factor does not only raise concerns about state sovereignty, but may also create legal uncertainty about the state competent to exercise enforcement jurisdiction. As the cooperation regime proposed by the Commission is based on the place where the service provider is offering its services, recourse to this ground for jurisdiction by third country legislation may result in a situation where a global provider of information and communication services must provide user data to law enforcement authorities of any country from whose territory these services can be accessed. As a consequence, **access to provider data** will be governed **by multiple jurisdictions** without the service provider or its customer being able to foresee the conditions and restrictions under the cooperation regime to be applied. Where minimum requirements of legal certainty and transparency are not met, the individual will not be able to exercise his right to data protection (Art. 8 CFR) and to decide on whether to make use of a particular information or communication service and to take the risk of his personal data being accessed by law enforcement authorities.[78]

Unlike reference to the location where the data is stored, other jurisdictional bases might provide less clear guidance on how to determine the country competent for enforcement jurisdiction. Thus, if enforcement jurisdiction shall be no longer linked to the location where the data is stored, it should not be based on a connecting factor that does not provide for a similar degree of legal certainty. In this regard, the rationale of territorial jurisdiction is still relevant and calls for a connecting factor that meets

[76] C. Burchard, "Der grenzüberschreitende Zugriff auf Clouddaten im Licht der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen", in *Zeitschrift für Internationale Strafrechtsdogmatik*, Vol. 13, 2018, p. 190, and p. 249, 250 ff.
[77] P.S. Bermann (note 74), 22 ff.
[78] C. Burchard (note 76), 252.

legitimate expectations of the citizens to be protected by the law of this particular jurisdiction:[79] If enforcement jurisdiction cannot be determined by the location where the data is stored, it appears reasonable to establish jurisdiction by reference to the place where the data is held (the establishment of the service provider).[80] Legitimate expectations of protection should be given particular weight where sensitive data shall be disclosed (content data and transaction data) whereas subscriber data may be subject to a less strict requirements.

Compared to the localisation via data storage or control, the connecting factor applied in the Commission's proposal appears rather broad, in particular with regard to service providers offering their services worldwide. The Commission's proposal addresses the **need for legal certainty** by defining the jurisdictional link as follows: A service provider offers services in the Union if it enables natural or legal persons to use its service in one or more MS(s) and has a **substantial link** to this MS respectively these MSs (Art. 2(4) draft regulation, Art. 2(3) draft directive). This definition corresponds to the interpretation of Art. 18(1)(b) CCC according to the Cybercrime Committee's guidance note (supra 2.1.1.). Accordingly, a substantial link shall be considered to exist where the service provider is established in the Union (Art. 2(4) draft directive), has a significant number or users in one or more MSs or targets its activities toward one or more MSs (by local advertising or advertising in a local language, by making an application ("app") available in the relevant national app store, providing customer service in a local language).[81] On the other hand, the provision of services in view of mere compliance with the prohibition to discriminate based on customers' nationality cannot be considered as targeting activities towards one or more MS(s).[82]

In addition, the scope of the Commission's proposal is limited to **data pertaining to services offered in the Union** (Art. 3(3) draft regulation). The new cooperation regime does not allow for access to provider data related to services offered exclusively outside the EU.[83] The proposal does not further elaborate on whether this restriction refers to an abstract category or type of services or to a concrete relationship to the customer to whom services are offered or provided. Only the latter interpretation will enable the user to foresee that his/her data will be subject to enforcement jurisdiction in the Union respectively the issuing MS. The fact that a certain category or type of service is offered in the Union does not seem to establish a sufficient jurisdictional link to personal data of customers or users receiving such services exclusively outside the EU (for instance using storage facilities in a cloud computing system). In this regard, a clarification of the scope of the new instruments should be considered, at least with regard to particular sensitive data (content and transactional data) the user legitimately expects to be stored in – and protected by – a certain jurisdiction (supra 4.1.1.).[84] With this proviso, the Commission's proposal establishes criteria that, strictly construed, allow for a determination of enforcement jurisdiction that meets basic requirements of legal certainty.

4.1.3. The pitfalls of unilateral cross-border access to provider data

Finally, the unilateral approach pursued in the Commission's proposal may bear considerable risks for the interests of the EU and its MSs and the rights of its citizens. These risks can be avoided by a

[79] See also Klip (note 70), 411 f.
[80] Klip (note 70), 412; see also Sieber (note 27), 144.
[81] Recital (13) draft directive.
[82] Recital (13) draft directive, referring to Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market, O.J. L 60 I/1.
[83] Recital (26) draft regulation.
[84] See also C. Burchard (note 76), p. 250.

multilateral approach that establishes a coherent framework for cross-border access to provider data and, thereby, provides more legal certainty in the relationship with third countries.[85]

International relations are based upon the principles of sovereign equality of states.[86] Establishing a unilateral regime of mandatory cooperation with foreign service providers, the EU and its MSs will have to accept similar models of enforcement jurisdiction applied by third countries to enable them to directly access data stored and processed in the EU. Moreover, the Commission's proposal might undermine MSs' objections to other instruments of extraterritorial enforcement (subpoena orders). On the other hand, direct cross-border enforcement may provoke counter-reactions such as **blocking statutes** that may lead to conflicting legal obligations and a fragmentation of the internet. Generally speaking, direct cross-border access to provider data may foster tendencies to unilateralism and **compromise the effective functioning of the existing multilateral framework of international cooperation**.[87] Ad-hoc involvement of the competent authorities in the state concerned may mitigate these potential effects of the Commission's proposal[88], but does not alter the fact that unilateral approaches carry the inherent risk of eroding international solidarity among states in international cooperation. These concerns have most recently been confirmed by the adoption of the US Cloud Act (supra 4.1.1.).[89]

Secondly, unilateral enforcement may have serious consequences for the protection of the **rights of EU citizens**. Moving away from the location of data as determining factor for establishing jurisdiction will not only path the way for cross-border access to provider data stored outside the EU, but indirectly **expose data stored in the Union to direct access by law enforcement authorities in third countries**.[90] The General Data Protection Regulation (GDPR)[91] lays down strict rules for the transmission of personal data to third countries (Art. 44 ff. GDPR), but it does not seem consistent to refer to the location of data in order to apply the EU data protection standard, but to consider this criterion wholly irrelevant as far as cross-border access to data is concerned.[92] Again, unilateral enforcement mechanisms will give rise to **conflicting obligations**, and service providers might be forced to produce personal data even if the requirements of the EU data protection standard are not met.[93] In its proposal, the Commission expected third countries to respect EU data protection standards and prohibitions on the disclosure of personal data[94], but, under the logics of a unilateral approach, this will be entirely left for the sovereign decision of the relevant third state.[95]

4.2. Relations between Member States

In contrast to the current framework of judicial cooperation within the EU, the Commission's proposal will enable the competent authority of issuing MS to adopt a production or preservation order that

[85] See also Commission, Technical Document (note 8), p. 44.
[86] Art. 2(1) of the Charter of the United Nations.
[87] C. Burchard (note 76), p. 254 f., referring to the concerns raised by former law enforcement, national security and intelligence officials in the *Microsoft Ireland* case.
[88] See for instance the Descartes-case where Dutch authorities accessed and copied data relating to child pornography stored on servers located in the US, Cybercrime Convention Committee (T-CY), Report of the Transborder Group (note 5), p. 35.
[89] German Bundesrat, decision of 6 July 2018, Drucksache 215/18, p. 11 ff.
[90] Commission, Technical Document (note 8), p. 37.
[91] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, O.J. L 119/1.
[92] C. Burchard (note 76), p. 201.
[93] C. Burchard (note 76), p. 254; see also the exception under Art. 49(1)2 GDPR.
[94] Commission, Proposal for a Regulation (note 10), p. 21.
[95] See with regard to the recently adopted US Cloud Act the German Bundesrat (note 89), p. 12.

produces a legally binding obligation in the territory of another MS. This transnational dimension of the new cooperation instruments may interfere with the territorial sovereignty of that MS. These concerns are connected to the legal basis of the proposed regulation (4.2.1.) and the state's responsibility to protect the fundamental rights of its citizens (4.2.2.).

4.2.1. Territorial sovereignty and the limits of the Union's legislative competence

Prima facie, state sovereignty seems to be a non-issue in the relations between MSs as far as MSs have conferred their sovereign powers on the EU. A new cooperation regime established by EU law, thus, cannot violate the sovereignty of the MS as long as there is a valid treaty basis for this legislation. This assumption, however, cannot be taken for granted, but requires further analysis, in particular where new cooperation instruments interfere with the territorial sovereignty of MSs.

The draft regulation is based on Art. 82(1) TFEU and is considered to implement the **principle of mutual recognition**.[96] In contrast to other mutual recognition instruments such as the EIO, the binding obligation of the EPOC and the EPOC-PR does not require prior recognition by the MS in which the order shall be executed; a "recognition" of the order is only foreseen where the addressee fails to comply with its obligation to execute the order and the judicial authority of the "enforcing" MS takes the necessary measures to enforce the order (Art. 14(2) draft regulation, supra 3.1.4.).[97] Thereby, the core of the Commission's proposal, a framework of direct cooperation between judicial authorities of the issuing MS and private companies in another MS, goes far beyond the well-established legislative practice and an understanding of mutual recognition of judicial decisions (Art. 82(1)2(a) TFEU) as cooperation between judicial or equivalent authorities of the MS (Art. 82(1)2(d) TFEU). The Commission's proposal suggests that the enforcing state generally recognizes any EPOC or EPOC-PR issued against an addressee located within its territory. Even though this concept has been applied in the framework of judicial cooperation in civil matters[98], it ignores the particularities of cooperation in criminal matters that is also reflected in the different wording of Art. 81(2)(a) and Art. 82(1)2(a) TFEU: Laying down "rules and procedures for ensuring recognition" would be superfluous if an involvement of the recognizing MS would not be required at all.[99] This understanding corresponds to the strict interpretation of Art. 82(1) TFEU taken by the Court of Justice in its opinion on the EU-Canada PNR agreement.[100]

The doubts on whether Art. 82(1) TFEU provides a legal basis for a mechanism of direct cooperation between law enforcement authorities and service providers find further support in **Art. 89 TFEU** that makes EU legislation on **extraterritorial operations of law enforcement authorities** subject to specific requirements. According to this treaty provision, the Union may lay down the conditions and limitations under which the judicial and police authorities of the Member States (Art. 82, 87 TFEU) may operate in the territory of another Member State. As such operations significantly interfere with the territorial sovereignty of the latter MS, the treaty provides for two safeguards: The operation must be

[96] Commission, Proposal for a Regulation (note 10), p. 5.
[97] Commission, Proposal for a Regulation (note 10), p. 3, 5.
[98] Art. 36(1) Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, O.J. L 351/1.
[99] See also the concerns raised by the German Bundesrat (note 89), p. 4; C. Burchard (note 76), p. 267.
[100] CJEU, Opinion 1/2015 of 26 July 2017, EU-Canada PNR Agreement, ECLI :EU:C:2017:592, para. 103 f.; see for the reference to this opinion in the context of the Commission's proposal: E. Sellier and A. Weyenbergh, "Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation", study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, PE 604.977, August 2018, p. 31.

carried out **in liaison and in agreement with the authorities of the MS whose territorial sovereignty is affected** (Art. 89 1 TFEU), and the adoption of the legislative measure requires a unanimous decision of the Council so that every MS has a veto in order to protect its territorial sovereignty (Art. 89 2 TFEU). The obligation of a service provider to comply with an EPOC or EPOC-PR issued in another MS interferes with the territorial sovereignty of that MS just as cross-border surveillance and hot-pursuit (Art. 40, 41 CISA) do, the prototypes of extraterritorial operations as set out in Art. 89 TFEU. As the competence to issue an EPOC or an EPOC-PR does not depend upon a connecting factor to the issuing MS, the addressee cannot be considered as a domestic service provider. The need for an involvement of the MS in which the order shall be executed has been discussed in the expert consultation process: Without express reference to Art. 40(2)(a), 41(1) CISA, the Commission considered an obligation to notify the MS whose sovereignty were affected by the production order.[101] However, it remained an open question whether the **notification** should serve mere information purposes or establish a need for the notified MS to agree to the measure; as the corresponding provisions in Art. 40, 41 CISA, only the latter mechanism could be considered to maintain the state's territorial sovereignty.[102] The concept does not appear in the final proposal, but was taken up by several MSs in the Council.[103]

4.2.2. Territorial sovereignty and fundamental rights

The principle of territorial sovereignty does not merely protect state interests, but first and foremost enables the state to effectively protect the rights of its citizens. Taking the state's obligation to provide effective protection of fundamental rights seriously, a cooperation regime that relieves the state from its responsibility must raise serious concerns.

The state's responsibility to protect its citizens against fundamental rights violations resulting from cross-border access to personal data has been highlighted by the German Constitutional Court in its ruling on Art. 32 CCC.[104] The Court dismissed the complaint for the sole reason that the applicants failed to substantiate the alleged violation of their fundamental rights, but a dissenting opinion came to the opposite conclusion and argued that the German legislature, by ratifying Art. 32 CCC, violated the applicant's privacy rights by authorising foreign authorities to access personal data without providing effective protection against violations of privacy rights resulting from such access.[105] Referring to the Constitutional Court's ruling, the Upper House of the German Parliament representing the states (Bundesrat), has raised similar objections to the Commission's proposal.[106] Since these concerns are rooted in the inherent connection of state sovereignty and **state responsibility to protect fundamental rights**, they do not reflect a merely national perspective (constitutional law), but are based on the shared responsibility of the Union and its MSs for ensuring effective fundamental rights protection.[107] The MS from whose territory personal data shall be transmitted to the issuing MS cannot be relieved from this responsibility, but must by itself ensure an adequate protection of privacy rights. This issue shall be further discussed in the following section on fundamental rights (infra 5.1.2.).

---

[101] Commission, Technical Document (note 7), p. 33.
[102] See also the German Bundesrat (note 89), p. 7.
[103] See the comments of the German, Latvian, Finnish and Swedish delegations in the Council, Council-Document No. 10470/1/18 of 28 June 2018, p. 10, 12, 14, 15.
[104] Bundesverfassungsgericht [German Federal Constitutional Court], Decision of 21 June 2016, 2 BvR 637/09, official court reports [BVerfGE], Vol. 142, p. 234, 249 ff.
[105] Dissenting opinion of Judge Huber, ibidem, at 257 ff.
[106] German Bundesrat (note 89), p. 6.
[107] C. Burchard (note 76), pp. 251, 259.

5. FUNDAMENTAL RIGHTS AND LEGAL CERTAINTY

KEY FINDINGS

- Establishing a mechanism of direct cooperation between the issuing authority and the service provider, the Commission's proposal deprives the individual of the protection by the traditional framework of cross-border cooperation and the cooperation obstacles applicable to that framework.
- Due to the sensitive nature of transactional and content data, access to such data is subject to formal and substantive requirements that vary from MS to MS. The Commission's proposal provides for an obligation to execute and enforce the production order even if the conditions set out by the law of the enforcing MS are not met, and thereby ignores the standard of protection under the *lex loci*. The threshold defined by the proposal (harmonised offence, minimum maximum penalty) does not ensure an equivalent level of protection. The disclosure of subscriber data does not meet similar concerns as such data is less sensitive and accessible via the European Investigation Order without regard to a particular threshold established by the law of the executing MS.
- The proposed cooperation mechanism relieves the enforcing MS from its protective function insofar as the production order is executed without enforcement being necessary. Instead, the issuing MS and the service provider are assigned with this function, but neither of them is in the position to ensure an equivalent protection of the users' privacy rights.
- The concentration of judicial review in the issuing MS raises similar concerns as it neglects the enforcing MS's responsibility to protect fundamental rights. Furthermore, judicial remedies available to the service provider are limited to enforcement proceedings and conflicting obligations, but do not entail a right to challenge before a court of the issuing MS the legality of the order.
- The Commission's proposal does not overcome the fragmentation of divergent national laws because the production and preservation orders to domestic service providers will remain subject to national law and the proposed cooperation regime still significantly refers to the national laws of the issuing and enforcing MS. The objective to establish a level playing field for service providers and to enhance legal certainty by harmonised rules on direct cooperation, however, must be balanced with the legitimate expectations of users and customers that human rights and privacy standards established by the national laws of criminal procedure will be maintained.

Due to the huge amount and the sensitivity of data processed and stored by service providers, the rules on access to provider data must include adequate safeguards for fundamental rights and freedoms of the persons concerned. The following section will analyse the impact to the Commission's proposal on the fundamental rights of service providers and the persons to whom the requested data relates (5.1.). The second part of this section shall discuss whether the new cooperation regime will overcome the fragmentation of divergent national laws and, thereby, improve legal certainty for businesses and service providers (5.2.).

5.1. The impact on the protection of fundamental rights

The analysis of the Commission's proposal has revealed that the new cooperation regime differs from the existing framework (the EIO in particular) in two respects: First, the proposal significantly reduces the grounds on the basis of which the execution or enforcement of the order may be refused (5.1.1.). Second, the intervention of the MS on whose territory the addressee of the EPOC or the EPOC-PR is located is limited to the enforcement stage (5.1.2.). The limited role of the enforcing MS has repercussions on the right to an effective judicial remedy (5.1.3.).

5.1.1. Access conditions and grounds for refusal

The Commission's proposal eliminates several refusal grounds aiming at protecting individual rights that are well-established in the current cooperation framework (for instance the double criminality requirement). Thereby, the individual is deprived of the protection under traditional MLA proceedings and/or mutual recognition instruments.

The need to respect the level of protection under the *lex loci* is addressed by the requirement that an EPOC must not be issued nor enforced if the requested data is protected by **immunities or privileges granted by the law of the enforcing MS** (Art. 5(7), Art. 14(2) draft regulation). However, unlike the EIO Directive (Art. 11(1)(h), supra 3.1.2), the proposal does **not** refer to the protection provided by **formal and substantive requirements for production orders** under the law of the MS where the service provider is addressed. As a consequence, the competent authority of the enforcing MS must enforce the order even if domestic law provides for a higher standard of protection than the law of the issuing MS.

These concerns are not merely theoretical as the formal and substantive requirements for production orders vary significantly from MS to MS. As far as **content or transactional data** is concerned, the applicable threshold may range from any criminal offence (France)[108] to serious offences or offences committed by means of telecommunication (Germany)[109], serious catalogue offences (the Netherlands[110]) or serious offences punishable by a custodial sentence of at least one year (Austria)[111]. On the other hand, a specific threshold does not apply as far as access to provider data is still subject to the general rules on search and seizure and on disclosure by production orders.[112] A similar **variety of national laws** exists with regard to the corresponding formal requirements: A production order may be issued by a public prosecutor or an investigating judge (France)[113] or require court authorisation (Austria, Germany)[114].

---

[108] Art. 60-1 and Art. 60-2 of the French Code of Criminal Procedure (Code de procédure pénal); see W.J. Maxwell, "Systematic Government Access to Private-Sector Data in France", in F.H. Cate and J.X. Dempsey (eds.), *Bulk Collection: Systematic Government Access to Private Sector Data*, 2017, Oxford University Press, p. 49, 51.

[109] § 100g(1) of the German Code of Criminal Procedure [Strafprozessordnung].

[110] Art. 126ng, Art. 67(1) of the Dutch Code of Criminal Procedure [Wetboek van Strafvordering].

[111] § 135(2) No 3 of the Austrian Code of Criminal Procedure [Strafprozessordnung].

[112] L. Bachmeier-Winter, "General Report: Section III – Criminal Procedure Information Society and Penal Law", *International Review of Penal Law*, Vol. 85, 2014, p. 75, 106. In Germany, access to content data (for instance an email) may be based on the general provisions, too (Bundesverfassungsgericht [German Federal Constitutional Court], Decision of 16 June 2009, 2 BvR 902/06, official court reports [BVerfGE] volume 124, p. 43); for a detailed analysis of the German provisions on the gathering of electronic evidence: C. Warken, "Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus – Teil 2", in *Neue Zeitschrift für Wirtschaftsstrafrecht*, Vol. 6, 2017, p. 329, 333 ff.; C. Warken, "Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus – Teil 3", in *Neue Zeitschrift für Wirtschaftsstrafrecht*, Vol. 6, 2017, p. 417 ff.

[113] W.J. Maxwell (note 108), p. 51.

[114] § 137(1)2 of the Austrian Code of Criminal Procedure [Strafprozessordnung]; § 101a(1)2 of the German Code of Criminal Procedure [Strafprozessordnung].

In addition, the **Directive on privacy and electronic communications**[115] calls upon the MS to ensure confidentiality of electronic communications and traffic data (Art. 5, 15). This obligation, read in the light of the right to privacy (Art. 7 CFR) and the right to protection of personal data (Art. 8 CFR), has been further elaborated in the case-law of the Court of Justice. As far as service providers are obliged to retain traffic and location data for law enforcement purposes, access to this data will allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained and, thus, must be subject to particularly high thresholds. Accordingly, law enforcement authorities may only order the production of retained data that is related to individuals suspected of having committed a **serious crime**.[116] As the concept of "serious crime" is not defined by EU law, it is for the national legislature to determine the conditions under which service providers must produce the requested data, and the definition of what constitutes a serious crime may vary from MS to MS.[117]

Instead of referring to the protection provided by the law of the enforcing MS, the Commission's proposal establishes a **minimum threshold** for issuing an EPOC (offence punishable by a custodial sentence of at least three years or a harmonised computer-related crime or terrorist offence, supra 3.1.2.). The reference to computer-related crimes corresponds to similar approaches in the national criminal justice systems, but is not strictly related to the gravity of the crime.[118] The minimum threshold (**maximum sentence of at least three years imprisonment**) corresponds to definitions of the concept of "serious crime" under national law that, according to case-law of the European Court of Human Rights, were considered capable of justifying an interference with the right to privacy.[119] Nevertheless, it must be doubted whether this requirement can ensure that a production order will be issued for the investigation and prosecution of serious crimes only. The penalty levels in the MSs' national criminal justice systems suggest that it will be rather the exception than the rule that a criminal offence will not meet the minimum threshold for issuing an EPOC. Contrary to the Commission's explanatory memorandum[120], the minimum maximum penalty of three years imprisonment does not exclude **petty offences** (simple theft, fraud, assault) from the scope of the EPOC.[121] Thus, a requirement that will be met by most offences under national law, cannot be considered an adequate threshold for particularly intrusive measures.[122] This assessment is confirmed by the fact that the the threshold proposed by the Commission has emerged from exceptions to the double criminality requirement (supra 3.1.2.) and hence from a restriction applicable to any criminal offence. As a result, the minimum threshold defined by the proposal even deprives the individual from the protection under the double criminality requirement because the production order must be executed and enforced irrespective of whether the crime investigated by the issuing MS constitutes a criminal offence under the law of the enforcing MS.[123]

As far as production of **subscriber data and access data** is concerned, similar concerns do not arise because the double criminality requirement and restrictions to serious offences have been waived for

[115] Directive 2002/58/EC (note 36), as amended by Directive 2009/136/EC (note 36).
[116] CJEU, Judgment of 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige* and *Watson*, paras. 99 f., 119.
[117] Ibidem, para. 118; AG Saugmandsgaard Øe, Opinion of 3 May 2018, Case C-207/16, *Ministerio Fiscal*, para. 95 ff., with regard to the implementation of the Directive into Spanish law.
[118] According to § 100g(2) of the German Code of Criminal Procedure [Strafprozessordnung], the service provider is obliged to disclose traffic data retained for law enforcement purposes only if a serious crime (a catalogue offence) is investigated; the provision does not apply to any crime committed by means of telecommunication.
[119] ECtHR, Judgment of 18 May 2010, Application No 26839/05, *Kennedy vs. United Kingdom*, paras. 159, 170.
[120] Commission, Proposal for a Regulation (note 10), p. 16.
[121] See for instance the maximum punishment for theft, fraud and assault according to §§ 223, 242, 263 of the German Criminal Code [Strafgesetzbuch] or Art. 222-11. 311-3, 313-1 of the French Criminal Code [Code pénal].
[122] See also the assessment of AG Saugmandsgaard Øe (note 117), para. 114 ff.
[123] German Bundesrat (note 89), p. 9.

the collection of subscriber data, including access data such as IP addresses (Art. 10(2), Art. 11(2) EIO Directive, supra 3.1.2.).[124] However, it must be maintained that access to this data is not limited by well-established obstacles to cross-border cooperation (see Art. 11(1)(d) and (e) EIO Directive).

5.1.2. The re-allocation of protective functions

The Commission's proposal does not only affect the standard of protection provided by the law of the enforcing MS, but also re-allocates the responsibilities for providing this protection in international cooperation. Since the role of the MS in which the service provider is addressed is strictly limited to enforcement, most orders will be executed without intervention of the "enforcing" MS. As a consequence, the **enforcing MS** will **not be able to exercise its protective function** as far as the service provider complies with the production order. Instead, the protective function is assigned to the **addressee of the order** and the competent authority in the **issuing MS**.

As far as the addressee of the order is concerned, there are considerable doubts whether **service providers** are in position to provide for effective human rights protection in the framework of international cooperation in criminal matters. The service provider is subject to an obligation to produce the requested data, and, unlike a public authority, runs the risk to be **subject to enforcement measures and sanctions in case of non-compliance**. The strict time-limits (6 hours in urgent cases) are likely to confront providers with serious difficulties in merely producing the requested data and will not allow for in-depth-assessment of human rights issues. Furthermore, the decision on whether or not to disclose the data may be subject to business considerations, and a human rights assessment requires financial and personal resources. A delegation of the state's responsibility for the protection of fundamental rights therefore requires a **detailed regulation of the service provider's responsibilities**, procedural safeguards (for instance the requirement of a reasoned decision) and supervision by the competent authority. As the mechanism proposed by the Commission lacks such a regulatory framework, it leaves a loophole in the protection of fundamental rights and bears the risk that the standard of protection under the law of the enforcing MS could not be maintained.[125]

In addition, the **protective function** of the service providers is rather **weak** because they are not obliged to assess whether the conditions for the execution of the order are met, but **"may" oppose** enforcement of the order. Moreover, the service provider is not even allowed to refuse to execute the order and to oppose its enforcement if the requested information is protected by a privilege or immunity under domestic law (Art. 8, Art. 14(4) draft regulation). Similarly, the refusal ground on the European *ordre public* is limited to **manifest violations of fundamental rights** that are apparent from the sole information contained in the order (Art. 14(4)(f), (5)(e) draft regulation; see supra 2.1.3.). As the certificate does not contain further information on the facts of the case, a human rights assessment will be hardly possible, and a request for additional information is not foreseen.[126]

As neither the enforcing MS nor the service provider can provide adequate protection of the users' privacy rights, the **issuing MS** is assigned with this task insofar as the competent authority has reasons

[124] German Bundesrat (note 89), p. 9; see for instance Art. 46bis of the Belgian Code of Criminal Procedure [Code d'instruction criminelle], Art. 126na(1) of the Dutch Code of Criminal Procedure [Wetboek van Strafvordering]; § 100j(1) of the German Code of Criminal Procedure [Strafprozessordnung].
[125] C. Burchard (note 76), pp. 260, 266; see also the concerns raised by the Finnish delegation in the Council, Council-Document 10470/1/18 REV 1 of 28 June 2018, p. 13; E. Sellier and A. Weyenbergh (note 100), p. 29 f.
[126] German Bundesrat (note 89), p. 6

to believe that the requested information is protected by privileges and immunities under the law of the MS where the service provider is addressed (Art. 5(7) draft regulation; supra 3.1.2.). This mechanism, however, does not provide adequate protection, either: The competent authority of the issuing MS usually **lacks the expertise to interpret and apply foreign law** and, as a rule, will not be aware of potential violations of immunities or privileges under the law of the enforcing MS. Furthermore, the protective function is closely linked to the state's interest to maintain the rule of law on its own territory (supra 4.2.2.). Conducting a criminal investigation, the issuing state pursues its own interests and **cannot guarantee an impartial and unbiased assessment** of the sovereign interests and the law of the enforcing MS.[127]

5.1.3. Judicial review

The re-allocation of protective functions under the new cooperation regime has implications for judicial review:

As far as the order is executed without recourse to the enforcement mechanism being necessary, the production of the requested data will not require the intervention of the competent authorities of the enforcing MS nor of its courts. Since the only coercive measure interfering with the rights of the user to which the requested data relates is the production order taken by the issuing authority, it is for the courts of the issuing MS to review the legality of the order. The **concentration of judicial review in the issuing MS** is inherent to the concept of a transnationally binding order and includes an assessment of immunities and privileges under the law of the enforcing MS (Art. 18 draft regulation, supra 3.1.5.). It should, however, be clarified, that the issuing authority shall inform the person concerned about the data production and the available remedies (supra 3.1.5.).

In the light of the foregoing observations on the responsibility of the MS where the order shall be executed (supra 4.2.2. and 5.1.2.), the concentration of judicial review in the issuing MS meets similar objections as the **shift of protective functions** from the executing authority to the issuing authority. If the law of the enforcing MS provides for immunities and privileges, it lies within the responsibility of that MS, its competent authorities and courts, to ensure that information protected by the corresponding provisions are not produced to the issuing MS.[128] This applies even more where the proposed cooperation regime are supplemented by a notification mechanism allowing the enforcing MS to object to or to agree with the execution of the order (supra 4.2.1.) because any such decision of an authority of the enforcing MS shall be subject to review by a domestic court.

As far as the addressee of the order is concerned, the Commission's proposal provides for judicial remedies in both the issuing and the enforcing MS. The need for judicial review in the enforcing MS is based on the rationale that an **enforcement decision** imposing a penalty on the addressee interferes with the fundamental rights of the latter and therefore must be **subject to judicial review** (Art. 14(10)2 draft regulation). The **review mechanism for conflicting obligations** (Art. 15, 16 draft regulation) follows a similar reasoning, referring to the service providers' risk of being sanctioned for non-compliance with the law of third countries or with the obligations under EU law (supra 3.1.5.). Nevertheless, in contrast to the individual user to which the requested data is related, the **service**

[127] German Bundesrat (note 89), p. 6 f.; C. Burchard (note 76), p. 266.
[128] See also E. Sellier and A. Weyenbergh (note 100), p. 30.

provider is not provided with a general legal remedy to challenge the legality of the order in the issuing MS (Art. 17 draft regulation, supra 3.1.5.).

Apparently, the underlying rationale of this restrictive approach is that there is no need for a legal remedy as long as the addressee of the measure is not subject to sanctions or other enforcement measures. This understanding, however, does not seem to be in conformity with the **right to an effective judicial remedy (Art. 47(1) CFR)** because the order imposes a legally binding obligation upon the addressee and thereby interferes with its fundamental rights. Therefore, the service provider has a legitimate interest to challenge the legality order even before enforcement proceedings are initiated. Judicial remedies against the enforcement decision is not equivalent to judicial review in the issuing MS because the grounds for refusal in enforcement proceedings do not fully correspond to the conditions for issuing an EPOC or EPOC-PR (supra 3.1.4.): The enforcing authority does not assess the legality of the EPOC under the law of the issuing MS, in particular whether the production order is proportionate and would be available in a comparable domestic case (Art. 5(2) draft regulation). Thus, without the right to challenge the legality of the order in the issuing MS, the service provider has **no legal remedy against an EPOC that has not been adopted in accordance with the law of the issuing MS**.

5.2. Fragmentation and legal certainty

According to the Commission, the new cooperation regime shall not only enhance cross-border access to provider data, but also establish a level playing field for service providers and ensure a better functioning of the internal market. A harmonised cooperation regime shall overcome the fragmentation of divergent national laws and, thereby, improve legal certainty for businesses and service providers.[129]

It cannot be denied that the Commission's proposal establishes a **harmonized set of rules** on which the new cooperation instruments are based, namely the formal and substantive requirements for the issuing of the order, the obligations of its addressee, enforcement and legal remedies (supra 3.1. and 3.2.). Furthermore, the cooperation regime shall be mainly based on a regulation that establishes uniform rules throughout the Union, without leaving a margin of appreciation to the MSs to implement these rules into national law. However, the MSs' **national laws** will still determine the service providers' cooperation obligations to a significant extent:

First, the new cooperation regime's **scope is limited to cross-border access** to provider data; it does not apply to production orders addressed to providers established or represented in the issuing MS (supra 3.1.1.). The Commission's proposal does not prevent the MSs from addressing service providers established in their territory (Art. 1(3) draft directive, supra 3.2.). Thus, the cooperation obligation of the service provider will depend upon whether the production order is issued by a domestic authority (national law) or by the authority of another MS (EU law).
Second, the new cooperation regime is not regulated by EU law only, but also **refers to the national law of the issuing MS**: An EPOC may only be issued if a similar measure would be available in a comparable domestic case (Art. 5(2) draft regulation), in other words: The substantive requirements (threshold, privileges and immunities) for a domestic production order apply accordingly. As a consequence, the range of the service provider's cooperation duties depends on the issuing MS. At first

[129] Commission, Proposal for a Directive (note 11), p. 3.

sight, the obligation to comply with the order is not limited by the law of the issuing state because the exhaustive list of grounds for non-execution (Art. 9, 10; Art. 14(4) and (5) draft regulation) does not refer to the law of the issuing MS. However, if EU law requires the EPOC to be issued in accordance with the law of the issuing MS, it would be contrary to the rule of law to force the service provider to comply with the order irrespective of whether or not this requirement is met (supra 5.1.3.).

Third, enforcement proceedings will be governed by the proposed regulation and **the law of the enforcing MS**. The latter will determine the penalties to be imposed for non-compliance with the order (Art. 14(10) draft regulation) and the **immunities and privileges** prohibiting the transmission of the requested data (Art. 14(2) and (9) draft regulation). In this regard, the applicable law will be determined by the model of one single legal representative of a service provider in the Union so that enforcement proceedings will be subject to the law of one MS only (the MS where the legal representative of the service provider is designated). Nevertheless, the proposal allows for enforcement by other MSs in which the service provider is established (Art. 1(3) draft directive; see also Art. 7(2)-(4) draft regulation) or for which the service provider has designated additional legal representatives (Art. 3(4) draft directive).

Thus, even though the Commission's proposal defines a common standard for cross-border access to provider data (judicial validation, minimum threshold for access to content and transactional data, conditions for execution and enforcement), it still allows MSs - albeit to a rather limited extent - to maintain their standards of protection applicable to the production of provider data. As a consequence, the **proposal will not fully overcome the current fragmentation** of divergent cooperation regimes in the MSs' criminal justice systems.

This fragmentation, however, follows from the limited scope of the Union's legislative powers. The competence under Art. 82(1) TFEU does not empower the Union to harmonise the formal and substantive requirements for investigative measures in the framework of domestic criminal proceedings. Due to the different legal traditions of the MSs, a **harmonisation of the law of criminal proceedings** is subject to rather strict requirements (Art. 82(2) TFEU). Above all, harmonising measures on aspects other than the admissibility of evidence, the rights of individuals or victims (Art. 82(2)(a)-(c) TFEU) require a prior decision of the Council, acting unanimously and with the Parliament's consent (Art. 82(2)(d) TFEU). In the absence of such a decision, the divergence of national laws on production and preservation orders will continue to exist.[130]

This divergence will inevitably affect the framework of cross-border cooperation. From the perspective of the issuing MS, it is a general rule that a mutual recognition instrument may only be issued if the corresponding measure would also be available in a comparable domestic case (Art. 5(2) draft regulation). The formal and substantive **requirements for the measure shall apply irrespective of whether the measure shall be carried out in or outside the territory of the issuing MS**. The provision on reimbursement of costs follows the very same reasoning (Art. 12 draft regulation). From the viewpoint of the executing (respectively enforcing) MS, the minimum requirements for an investigative measure (for instance a catalogue offence) define the level of protection that should be maintained in domestic criminal proceedings as well as in cross-border cooperation. In the

[130] For an overview on the divergence of the MSs' laws on investigative measures in criminal proceedings see E. Sellier and A. Weyenbergh (note 100), p. 21 ff.

Commission's proposal, this rule is reflected in the protection of immunities and privileges (Art. 14(2), (9) draft regulation).

For these reasons, the divergence of the MSs' laws is inextricably linked to maintaining an **equal level of protection in both domestic criminal proceedings and cross-border cooperation**. The Commission's proposal itself illustrates that harmonisation always bears the risk of lowering the standards established by national law. The service providers' interest in a level playing field established by a fully harmonised cooperation regime must be balanced with the **citizens' fundamental rights and their interest in being protected by the existing national standards**. Whereas the Commission's proposal does not even mention the legitimate expectations of users and customers, it lays a strong emphasis on the service providers' interest in legal certainty, and providers may even choose the jurisdiction or – if they designate additional legal representatives (Art. 3(4) draft directive) – the jurisdictions in which they will execute an EPOC or an EPOC-PR (supra 3.2.).Admittedly, fragmentation may have a negative impact on legal certainty for service providers, but citizens may nonetheless legitimately expect law enforcement authorities to be bound by the rules and safeguards under domestic law of criminal proceedings even if they act in the framework of cross-border cooperation, be it as issuing or enforcing authority. The objective to enhance legal certainty for service providers in the Union should not be pursued at the expense of the fundamental rights of users.

6. CONCLUSIONS AND RECOMMENDATIONS

6.1. Conclusions

The comparison with the existing framework of transnational evidence-gathering has clearly revealed the added value of the Commission's proposal on cross-border access to electronic evidence. Establishing a mechanism of **direct cooperation** between the MSs' law enforcement authorities and services providers offering their services in the Union, the new rules will avoid slow and cumbersome MLA proceedings and enable the competent authorities to access provider data more quickly and effectively. Nevertheless, the framework of international cooperation has improved significantly, and the **EIO**, as a new instrument for transnational evidence-gathering, has removed several obstacles to cross-border cooperation and **streamlined proceedings** by standardised forms and strict time-limits. In particular, the execution of an EIO issued for the production of subscriber data is not subject to the double criminality requirement nor to particular thresholds under the law of the executing MS (for instance catalogue offences). On the other hand, the EIO **still requires recognition and execution** by another MS whereas direct cooperation will render the involvement of the executing MS superfluous or, more precisely, limit such an involvement to enforcement proceedings. Thus, **direct cooperation** as proposed by the Commission **will save time and resources**.

The added value of the new cooperation regime, however, has its downside. The Commission's proposal extends enforcement jurisdiction to service providers established and data stored in non-Member States, and this **unilateral approach** may have a **negative impact on the functioning of the framework of international cooperation with third states**, give rise to conflicts of enforcement jurisdiction and **conflicting obligations of service providers** and create **legal uncertainty** for both service providers and users. Moreover, direct cooperation will affect the **territorial sovereignty of the MS** in which the service provider shall execute the new cooperation instruments (EPOC, EPOC-PR) and, thereby, ignores that MS's responsibility for an effective protection of fundamental rights within its territory.

The proposed cooperation mechanism does not provide for an adequate protection of fundamental rights, but **deprives the individual of the protection provided by the traditional framework** of international cooperation: The Commission's proposal eliminates a number of cooperation obstacles aiming at the protection of human rights (for instance the double criminality requirement). Most of all, the proposal establishes an obligation to produce content data and transactional data even if the **threshold set out by the law of the enforcing MS** are not met (serious offence, catalogue offence), and thereby ignores the standard of protection under the *lex loci*. As far as fundamental rights standards are maintained (*ordre public* clause, immunities and privileges under the law of the enforcing MS), the **protective function is not exercised by the MS in whose territory the order shall be executed**, but by the service provider and/or the competent authority of the issuing MS neither of which is in position to ensure adequate protection. In addition, the re-allocation of protective functions has implications for the right to **judicial review** as judicial remedies of the individual whose data has been transmitted are concentrated in the issuing MS; the proposal does not provide for a right to challenge the disclosure before a court of the enforcing MS, claiming that the data is protected by a privilege under the law of the enforcing MS. The **service provider** is provided with legal remedies in the enforcing MS (enforcement proceedings) and in the issuing MS (review procedure in case of

conflicting obligations), but **may not challenge the legality of the order under the law of the issuing MS**.

The Commission's proposal establishes a harmonised framework for direct cooperation between law enforcement authorities and service providers in the AFSJ. The new framework, however, will **not overcome the fragmentation and divergence of the MSs' laws** on the preservation and production of electronic evidence. Production and preservation orders to domestic service providers will remain subject to national law and the proposed cooperation regime still significantly refers to the national laws of the issuing and enforcing MS. Further harmonisation would require a legislative measure harmonising the laws of criminal procedure (the formal and substantive requirements for investigative measures such as production and preservation orders). Taking the different traditions of the MSs and the requirements of the applicable treaty basis (Art.82(2)(d) TFEU) into consideration, such a measure does not appear feasible for the time being. As a consequence, the divergence of national laws on (domestic) access to provider data will continue to exist and give rise to **legitimate expectations of users and customers** that **human rights and privacy standards established by the *lex loci*** will be maintained. These legitimate expectations should not be predominated by the interest in a common level playing field for services providers and a better functioning of the internal market.

6.2. Recommendations

6.2.1. Direct cooperation and European Investigation Order

The added value of the new cooperation regime (quick and effective access to provider data) is mainly based on the abolition of cooperation obstacles and procedures ensuring effective protection of fundamental rights. Since the EIO Directive has maintained most of the corresponding rules and safeguards, but, at the same time, has facilitated and streamlined cross-border access to electronic evidence, subscriber data in particular, the added value of direct cooperation with service providers might be outweighed by a less effective protection of fundamental rights. In the legislative process, the ongoing implementation should be carefully observed in order to re-consider whether and to what extent **recourse to the EIO** might be an **alternative option** to the EPOC or the EPOC-PR; this applies in particular to the disclosure of content and transactional data. In any case, the proposal should clarify the relationship between the EIO on one hand, and the new cooperation instruments on the other.

6.2.2. Unilateral enforcement and multilateral solutions

To avoid or at least mitigate the negative consequences of the unilateral approach pursued by the Commission's proposal, the new cooperation regime should be supplemented by and coordinated with **bi- and multilateral agreements**, in particular the emerging second additional protocol to the CCC that will provide multilateral framework for the cooperation with non-Member States. A multilateral approach may also provide for solutions to conflicting obligations. As ubiquitous enforcement jurisdiction will give rise to **legal uncertainty**, it should be based upon a connecting factor that enables the individual to foresee that his/her data will be subject to enforcement jurisdiction in the Union respectively the issuing MS. Thus, if jurisdiction is not established via the location where the data is stored or where the service provider is established, the **connecting factor should be strictly construed**. To that end, the material scope of the Commission's proposal (data pertaining to services offered in the Union, Art. 3(3) draft regulation), should be defined more precisely **by referring to the customer(s) to whom services are offered or provided**.

6.2.3. Strengthening the role of the enforcing MS

The territorial sovereignty of the enforcing MS and its responsibility for protecting human rights on its territory call for a mechanism involving that MS before the order is executed. In analogy to the rules on cross-border surveillance and hot pursuit (Art. 40, 41 CISA), the new cooperation regime should provide for a **notification** of the MS in whose territory the service provider is addressed and, thereby, enable the competent authority of that **MS to take a decision on whether or not the order shall be executed**. Thereby, the "executing" (formerly the enforcing) MS will be able to ensure that the level of protection provided by its domestic law (for instance by privileges and immunities) is maintained (see also 6.2.4.).

6.2.4. Maintaining high standards of protection

The new cooperation regime should maintain the high standard of protection as defined by the EIO Directive. As a matter of principle, cross-border access to provider data should be subject to the same conditions as any other investigative measure, including the **refusal grounds** according to Art. 11(1)(d) and (e) EIO Directive. Content data and transactional data shall be disclosed and transmitted to the issuing authority only if the **double criminality requirement** is met (Art. 11(1)(g) EIO Directive)and if a corresponding production order would be available under the law of the MS where the order shall be executed, in other words, the corresponding **restrictions (catalogue offence, serious offence)** shall apply accordingly (Art. 11(1)(h) EIO Directive). To that end, the definitions of the different categories of data should be refined as well (supra 3.1.1.).

6.2.5. Ensuring effective judicial review

Since the **service provider's right to** an effective judicial remedy (Art. 47(1)1 CFR) entails a right to **challenge the legality of the EPOC / the EPOC-PR**, the proposal should clarify that judicial review in the issuing MS is not limited to conflicting obligations (Art. 15, 16 draft regulation). As a consequence of the recommended notification procedure (supra 6.2.3.), the decision on the execution of the order shall be subject to judicial review by a court of the "executing" (formerly the enforcing) MS. Thus, the **individual** to whom the requested data pertains shall have a **judicial remedy** in the issuing MS (Art. 17 draft regulation) and **in the executing MS** (see also Art. 14 EIO Directive), and he/she shall be informed about the data production and the available remedies in both MS (supra 5.1.3.).

REFERENCES

EU documents

European Commission

- Commission, Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code, COM (2016) 590 final/2 of 12 October 2016.
- Commission, Non-paper: Progress report following the Conclusions of the Council of the European Union on improving criminal justice in cyberspace, Council Doc. No. 15072/16cd, 2 December 2016.
- Commission, Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, 22 May 2017.
- Commission, Technical document: Measures to improve cross-border access to electronic evidence for criminal investigations following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace, Council Doc. No. 9542/17, 22 May 2017.
- Commission, Staff Working Document, Impact Assessment, SWD (2018) 118 final, 17 April 2018.
- Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Order for electronic evidence in criminal proceedings, COM (2018) 225 final, 17 April 2018.
- Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM (2018) 226 final, 17 April 2018.

Council of the EU

- Council, Conclusions on improving criminal justice in cyberspace, 9 June 2016, Council Doc. No. 10007/16.
- Council, Compilation of Member States comments on the Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters, Council-Document No. 10470/1/REV 1 of 28 June 2018.

European Parliament

- European Parliament, Resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)), P8_TA(2017)0366.

EU secondary law

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, O.J. L 178/1.
- Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, O.J. L 149/1.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J. L 201/37.
- Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, O.J. L 196/45.
- Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, O.J. L 350/72.
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, O.J. L 337/11.
- Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, O.J. L 335/1.
- Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, O.J. L 351/1.
- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, O.J. L 218/8.
- Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, O.J. L 130/1.
- Directive (EU) 2015/1535 of the European Parliament and the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification), O.J. L 241/1.

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, O.J. L 119/1.

- Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, O.J. L 88/6.

- Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market, O.J. L 60 I/1.

Council of Europe treaties and documents

- European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 (ETS No. 30).

- Council of Europe, Convention on Cybercrime of 23 November 2001 (ETS No. 185).

- Council of Europe, Explanatory report to the Cybercrime Convention of 23 November 2001 (ETS No. 185).

- Cybercrime Convention Committee (T-CY), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, Transborder access and jurisdiction: What are the options?, Report of the Transborder Group, adopted by the T-CY on 6 December 2012, T-CY (2012)3.

- Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 3, Transborder access to data (Article 32), adopted by the 12th Plenary of the T-CY on 2–3 December 2014, T-CY (2013)7 E.

- Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 10, Production orders for subscriber information (Article 18 Budapest Convention), adopted by the T-CY following the 16th plenary by written procedure on 1 March 2017, T-CY (2015)16.

- Cybercrime Convention Committee (T-CY), Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, approved by the 17th Plenary of the T-CY on 8 June 2017, T-CY (2017)3.

Recent national legislation

Germany

- Network Enforcement Act ("Netzwerkdurchsetzungsgesetz") of 1 September 2017, Bundesgesetzblatt 2017, part I, p. 3352.

United States of America

- Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 23 March 2018 (H.R. 4943).

Court decisions and opinions

European Union

- CJEU, Judgment of 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige* and *Watson*.
- AG Saugmandsgaard Øe, Opinion of 3 May 2018, Case C-207/16, Ministerio Fiscal.

European Court of Human Rights

- ECtHR, Judgment of 18 May 2010, Application No 26839/05, Kennedy vs. United Kingdom.

League of Nations

- Permanent Court of International Justice, Judgment of 7 September 1927, Ser. A no. 10.

Belgium

- Hof van Cassatie [Belgian Court of Cassation], Judgment of 1 December 2015, P.13.2082.N, Yahoo.

Germany

- Bundesverfassungsgericht [German Federal Constitutional Court], Decision of 16 June 2009, 2 BvR 902/06, official court reports [BVerfGE] volume 124, p. 43.
- Bundesverfassungsgericht [German Federal Constitutional Court], Decision of 21 June 2016, 2 BvR 637/09, official court reports [BVerfGE], Vol. 142, p. 234.

Ireland

- Supreme Court of Ireland, 25 January 2013, Walsh v. National Irish Bank, Appeal No. 267/2007, [2013] 1 ESC 2.

United States of America

- US Supreme Court, 15 June 1987, . Societe Nationale Industrielle Aerospatiale et al. v. United States District Court for the Southern District of Iowa, 482 U.S. 522 (1987).

- US Supreme Court, 17 April 2018, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).
- US Court of Appeals, Ninth Circuit, Order of 3 June 1994, Opinion of 7 November 1994, In re Grandjury Proceedings, Marsoner v. U.S. 40 F 3d 959 (9th cir. 1994).
- US Court of Appeals, Second Circuit, 9 December 2016, In the matter of a Warrant to Search a Certain E-mail Account Microsoft v. US 829 F.3d 197 (2nd Cir. 2016).

Literature

- L. Bachmeier-Winter, "General Report: Section III – Criminal Procedure Information Society and Penal Law", in *International Review of Penal Law*, Vol. 85, 2014, p. 75.
- P.S. Bermann, "Legal Jurisdiction and the Deterritorialization of Data", in *Vanderbilt Law Review*, Vol. 71, 2018, p. 11.
- D. Brodowski, "Transnational Organised Crime and Cybercrime" in P. Hauck and S. Peterke (ed.), *International Law and Transnational Organised Crime*, Oxford University Press, 2016, p. 352.
- C. Burchard, "Der grenzüberschreitende Zugriff auf Clouddaten im Licht der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen", in *Zeitschrift für Internationale Strafrechtsdogmatik*, Vol. 13, 2018, p. 190, and p. 249.
- R.J. Currie, "Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the *Microsoft Ireland* Case the «Next Frontier»?", in *The Canadian Yearbook of International Law*, Vol. 54, 2017, Cambridge University Press, p. 63.
- J. Daskal, "The Un-Territoriality of Data", in *Yale Law Journal*, Vol. 125, 2015–2016, p. 326.
- P. de Hert, C. Parlar, and J. Saifert, "The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law", in Computer Law & Security Review, Vol. 34, 2018, p. 327.
- A. Klip, "Section IV – International Criminal Law. Information Society and Penal Law – General Report", in *International Review of Penal Law*, Vol. 85, 2014, p. 381.
- B.J. Koops and M. Goodwin, "Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities International Law", in Tilburg Law School Research Paper No. 5/2016, 2014.
- W.J. Maxwell, "Systematic Government Access to Private-Sector Data in France", in F.H. Cate and J.X. Dempsey (eds.), *Bulk Collection: Systematic Government Access to Private Sector Data*, 2017, Oxford University Press, p. 49.

- M. Schaub, "Zur völkerrechtlichen Zulässigkeit des amerikanischen Editionsbefehls an die UBS im Streit um die Kundendaten", in *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, Vol. 71, 2011, p. 807.

- E. Sellier and A. Weyenbergh, "Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation", study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, PE 604.977, August 2018

- U. Sieber, "Straftaten und Strafverfolgung im Internet: Gutachten C zum 69. Deutschen Juristentag", in Deutscher Juristentag (ed.), *Verhandlungen des 69. Deutschen Juristentages – München 2012*, Vol. 1 (Gutachten), C.H.Beck, 2012, p. 145.

- C. Warken, "Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus", in *Neue Zeitschrift für Wirtschaftsstrafrecht*, 2017, p. 289, p. 329, p. 417, and p. 449.

Other

- Brief for France as Amicus Curiae Judicial and Similar Proceedings: United States: Supreme Court Proceedings in Societe Nationale Industrielle Aerospatiale et al. v. United States District Court for the Southern District of Iowa, International Legal Materials 25 (1986), p. 1519.

- Brief for Federal Republic of Germany as Amicus Curiae Judicial and Similar Proceedings: United States: Supreme Court Proceedings in Societe Nationale Industrielle Aerospatiale et al. v. United States District Court for the Southern District of Iowa, International Legal Materials 25 (1986), p. 1539.

- German Bundesrat, decision of 6 July 2018, Drucksache 215/18.

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee, analyses the added value and the shortcomings of the Commission's proposals on cross-border access to electronic evidence, with a special focus on the proposals' implications for territoriality and state sovereignty and fundamental rights of service providers and users.

PE 604.989

Print ISBN 978-92-846-3862-8 | doi: 10.2861/38083 | QA-06-18-084-EN-C
PDF ISBN 978-92-846-3861-1 | doi: 10.2861/247211 | QA-06-18-084-EN-N